

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-308564

(43)Date of publication of application : 05.11.1999

(51)Int.Cl.

H04N 5/91
G09C 5/00
H04N 5/765
H04N 5/781
H04N 5/92

(21)Application number : 10-109352

(71)Applicant : OLYMPUS OPTICAL CO LTD

(22)Date of filing : 20.04.1998

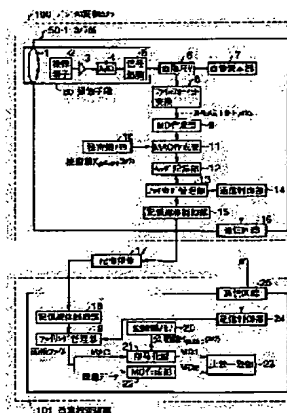
(72)Inventor : KONDO TAKASHI
HIGURE MASAKI
KOMIYA YASUHIRO
YAMADA HIDETOSHI

(54) DIGITAL EVIDENCE CAMERA SYSTEM, DECODING KEY ACQUISITION REGISTRATION SYSTEM AND DIGITAL IMAGE EDIT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a digital evidence camera system where evidence capability of a digital image is enhanced and an encrypted key is managed at a very high security level.

SOLUTION: The digital evidence camera system detects falsified image data obtained by photographing an object with a camera and consists of a camera section 50-1 provided with an image pickup means 60 that photographs an object and with a MAC generating section 11 that generates falsification detection data (MAC) from image data by photographing by using a secret key set in advance and of a falsification check device 101 that uses a public key corresponding to the secret key to decode the data MAC and checks whether or not the image data are falsified based on the decoding result.



LEGAL STATUS

[Date of request for examination]

20.04.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

*** NOTICES ***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. **** shows the word which can not be translated.

3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The image pick-up section for being the digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, the camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption -- since -- the digital of-evidence camera system characterized by becoming.

[Claim 2] The image pick-up section for being the digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, The camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption, since -- the alteration supervision mode as which, as for said camera, said image data detects whether it was altered or not -- in addition, with the secure mode in which encryption to the image data transmitted to said alteration detection section from said camera is performed It has the digital-watermarking mode which embeds digital-watermarking data at image data, and the normal mode which performs the usual photography without using a security function. The digital of-evidence camera system characterized by having the mode selection section for choosing the mode of at least one request from these modes.

[Claim 3] The decryption key storage section memorized in accordance with the 1st decryption key corresponding to the 1st encryption key generated by equipment corresponding to the identifier of a proper, and this identifier, The decryption key output section which creates the data for alteration detection about said 1st decryption key using the 2nd encryption key, and is outputted in accordance with this data for alteration detection, and said 1st decryption key, A preparation ***** server and the decryption key storage section which memorizes said 1st decryption key acquired from said decryption key server through means of communications etc., Said data for alteration detection supplied from said decryption key server through means of communications etc. are decrypted using the 2nd decryption key corresponding to said 2nd encryption key. the decryption key acquisition section equipped with the alteration detection section which detects whether said 1st decryption key was altered based on the result of this decryption -- since -- decryption key acquisition / registration system characterized by becoming.

[Claim 4] With the filing Management Department which is the digital image edit system into which image data is edited, and does filing management of the image data inputted through the image input section while detecting the alteration of image data While decrypting the 1st data for alteration detection beforehand given to said image data using the decryption key corresponding to the encryption key used when creating this data for alteration detection The alteration detection section which detects the

alteration condition of image data by comparing this the 1st decoded data for alteration detection and said image data, To said image data from the edited image data to which various image processings were performed by the image editorial department which performs various kinds of image processings, and said image editorial department, and the data of the edit hysteresis by said image editorial department the renewal section of an image file which creates the 2nd data for alteration detection using an encryption key other than said encryption key, and adds this to said edited image data -- since -- the digital image edit system characterized by becoming.

[Translation done.]

*** NOTICES ***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a digital of-evidence camera system, decryption key acquisition / registration system, and a digital image edit system.

[0002]

[Description of the Prior Art] The photograph analogically recorded on the film and media of the former, for example, a camera, and voice are used as what has the certification force in a trial etc. By advance of digital technique in recent years, the equipment which records an image and voice as digital data has spread. According to such digitization, the advantage which does not deteriorate even if it copies and which can be quickly distributed using a communication line in which processing and edit of the contents of information can be performed further easily is acquired. However, I hear that that processing and edit are easy can alter the contents of information easily by one side, there is, and room to suspect weight of the evidence as information is produced. Therefore, in order to enable it to use a digital image and voice as a piece of evidence, it is required to have the function to prevent the alteration of digital data by a certain approach. The camera which has such a prevention function is called the digital camera of evidence.

[0003] In order to realize this digital camera of evidence, it considers applying the electronic signature technique generally used by the communication link etc. Two keys used as a pair are used in an electronic signature system. One is called a private key with the key for encryption, and another side is called a public key with the key for a decryption. It is enciphered using a private key and digital data is decrypted using a public key. Although a tropism function is used on the other hand in quest of a public key from a private key, on the other hand, this thing [asking for a private key] is mathematical very difficult from the public key conversely with the property of a tropism function. While it needs to be severely managed so that no men other than an owner can use a private key by any means, generally a public key is exhibited so that anyone can use.

[0004] The approach of alteration detection is a transmitting side and creates the code first called a

message digest (Message Digest, following, MD) using a Hash Function etc. from the target digital data. If the method of extracting MD from the target digital data is exhibited and there are original data, anyone can extract MD. Incidentally, MD has the property in which a value changes a lot, when the original digital data differ from the good and known property.

[0005] Next, extracted MD is enciphered using a private key and he is a message authentication child (Message Authentication Code, following, MAC) about this. It carries out and transmits to the other party with original data. Here, the public key used as a private key and a pair shall be certainly passed to the addressee (an addressee may cross to the 3rd person's hand that what is necessary is just to surely have obtained the key).

[0006] In order to investigate that original data are not altered, first, a Hash Function etc. is used for a receiving side from original data, and it asks for MD'. Next, MAC is decrypted using a public key, MD is calculated, and it investigates whether this MD and MD' are in agreement. Even if original data are altered by the 3rd person, since the 3rd person does not have a private key, he cannot create MAC which can be decrypted with a public key, but becomes a different value from MD and MD'. This shows that original data were altered by the 3rd person.

[0007]

[Problem(s) to be Solved by the Invention] As described above, in order to detect the alteration of digital data, an electronic signature technique is applicable. However, when the approach of alteration detection which was described above was adopted as a digital camera of evidence, although it did not reveal by any means, conventionally, it was not easy to manage this private key on high security level, therefore, as for the private key as an encryption key, it was not able to heighten the weight of the evidence of a digital image.

[0008] Moreover, in the case of an image, there is the need of processing a data compression, field logging, insertion of a caption, etc. on the property of data, in many cases, but conventionally, by the approach of the electronic signature applied to document data, if it changes even when the contents of data are slight, it will be considered that data were altered. Therefore, in the conventional electronic signature system, required edit was not completed at all on the property of the above image data.

[0009] The place which this invention is made paying attention to such a technical problem, and is made into the purpose The digital of-evidence camera system which can heighten the weight of the evidence of a digital image, and can manage an encryption key on very high security level, Decryption key acquisition - It is offering a registration system, and even if it edits compression which is further needed on the property of an image, field logging, insertion of a caption, etc., it is in offering the digital image edit system which can maintain the weight of the evidence of a digital image.

[0010]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the 1st invention The image pick-up section for being the digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, Said data for alteration detection are decrypted using the camera to provide and the decryption key corresponding to said encryption key, and it consists of the alteration detection section which detects whether said image data was altered based on the result of this decryption.

[0011] Moreover, the image pick-up section for the 2nd invention being a digital of-evidence camera system which detects the alteration of the image data which picturized the photographic subject with the camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, Said data for alteration detection are decrypted using the camera to provide and the decryption key corresponding to said encryption key. It consists of the alteration detection section which detects whether said image data was altered based on the result of this

decryption. Said camera Whether said image data was altered to the alteration supervision mode to detect In addition, the secure mode in which encryption to the image data transmitted to said alteration detection section from said camera is performed, It has the digital–watermarking mode which embeds digital–watermarking data at image data, and the normal mode which performs the usual photography without using a security function, and has the mode selection section for choosing the mode of at least one request from these modes.

[0012] The 3rd invention is decryption key acquisition / registration system. To equipment Moreover, the identifier of a proper, The decryption key storage section memorized in accordance with the 1st decryption key corresponding to the 1st encryption key generated corresponding to this identifier, The decryption key output section which creates the data for alteration detection about said 1st decryption key using the 2nd encryption key, and is outputted in accordance with this data for alteration detection, and said 1st decryption key, A preparation ***** server and the decryption key storage section which memorizes said 1st decryption key acquired from said decryption key server through means of communications etc., Said data for alteration detection supplied from said decryption key server through means of communications etc. are decrypted using the 2nd decryption key corresponding to said 2nd encryption key. It consists of the decryption key acquisition section equipped with the alteration detection section which detects whether said 1st decryption key was altered based on the result of this decryption.

[0013] With moreover, the filing Management Department which the 4th invention is a digital image edit system into which image data is edited while detecting the alteration of image data, and does filing management of the image data inputted through the image input section While decrypting the 1st data for alteration detection beforehand given to said image data using the decryption key corresponding to the encryption key used when creating this data for alteration detection The alteration detection section which detects the alteration condition of image data by comparing this the 1st decoded data for alteration detection and said image data, To said image data from the edited image data to which various image processings were performed by the image editorial department which performs various kinds of image processings, and said image editorial department, and the data of the edit hysteresis by said image editorial department The 2nd data for alteration detection is created using an encryption key other than said encryption key, and it consists of the renewal section of an image file which adds this to said edited image data.

[0014]

[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained to a detail with reference to a drawing. Drawing 1 is drawing showing the digital of–evidence camera structure of a system concerning the 1st operation gestalt of this invention, and consists of a digital camera 100 of evidence and alteration test equipment 101. The camera section 50–1 of the digital camera 100 of evidence has the image pick–up means 60 which consists of a taking lens 1, an image sensor 2, amplifier 3, A/D converter 4, and the signal–processing section 5. The photographic subject image which carried out incidence through the taking lens 1 is picturized by the image sensor 2. The electrical signal acquired by this image pick–up is amplified by the amplifier 3, and after being changed into a digital signal in the A/D–conversion section 4 and performing signal processing predetermined in the signal–processing section 5, it is memorized as image data in an image memory 6. The image data memorized in this image memory 6 is displayed on the image display section 7 if needed.

[0015] The image data memorized in the image memory 6 is changed into the graphics format of criteria, such as JPEG and TIFF, in the file–format–conversion section 8. Thereby, the file format by which the data of header information were added to image data is created ((A) of drawing 2). Next, in MD creation section 9, MD is created by applying predetermined functions, such as a Hash Function, to the data of the whole also including image data or a header ((B) of drawing 2). Next, in the MAC creation section 11, MAC is created by enciphering MD using the private key Kprivate (camera) memorized beforehand in the private key memory 10 ((C) of drawing 2). Next, at the header Records Department 11, created MAC is

stored in an image header ((D) of drawing 2). At the filing Management Department 13, file management to the image file of the file format created by doing in this way is performed.

[0016] Such an image file demounts by control of the storage control section 15, and in order to detect whether it was altered while having been transmitted through the communication line 16 by control of the communications control section 14 while being memorized and carried by the possible storage 17 or, alteration detection equipment 101 is used.

[0017] That is, the image file memorized by the storage 17 with which alteration test equipment 101 was equipped is read to the filing Management Department 19 by control of the storage control section 18. Or the image file concerned is sent to the filing Management Department 19 through a communication line 25 by control of the communications control section 24. At the filing Management Department 19, an image file is divided into MAC and image data (header information other than the image data itself, such as JPEG and TIFF, may be included in this image data), MAC is inputted into the decryption section 21, and image data is inputted into MD creation section 22.

[0018] In the decryption section 21, MD1 is generated by decrypting MAC using the public key Kpublic (camera) memorized beforehand in the public key memory 20. This public key Kpublic (camera) and the above mentioned private key Kprivate (camera) are keys which serve as a pair in encryption/decryption processing. On the other hand, in MD creation section 22, MD2 is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23, when MD1 is compared with MD2 and both are not in agreement, it can judge with the image file having been altered by the 3rd person.

[0019] According to the above-mentioned 1st operation gestalt, the data (MAC) for alteration detection are created using the encryption key in a camera from image data, and it can check whether image data is altered by writing in this data for alteration detection in an image file, for example, the header information of an image. The weight of the evidence of the digital image it was presupposed that it was inferior of a digital image by this compared with the image conventionally photoed using the film can be heightened.

[0020] Moreover, by this operation gestalt, although the encryption key for creating the data for alteration detection is not revealed outside by any means including a camera user, since the encryption key for creating the data for alteration detection is beforehand stored in the memory area in a camera, it can manage an encryption key on very [in hard] high security level.

[0021] Next, the digital camera of evidence which has various kinds of modes (multimode) as the 2nd operation gestalt of this invention is explained. Here, the function of the request according to the purpose of using a camera can be set up by equipping a camera with the optional feature in the following various modes. Various modes are secure modes which encipher an image file here, the usual photography mode in which a security function is not used, the alteration supervision mode which gives alteration detection data to the photoed image file and the digital-watermarking mode which records the photoed copyright information on a photograph on an image file as digital watermarking, when saving an image file further at a dismountable storage, or when transmitting an image file using communication facility.

[0022] Hereafter, with reference to drawing 3 , it explains to a detail further. What has the same reference number as drawing 1 in drawing 3 shall have the same function. In the digital camera 102 of evidence which consists of the camera section 50-2 in this operation gestalt, a user can choose [from] the desired mode among various kinds of modes described above in the mode selection section 31.

[0023] For example, when normal mode is chosen, the image data which picturized the photographic subject with the image pick-up means 60, and was obtained is memorized in an image memory 6. Especially in this mode, security mode does not work, but format conversion is carried out in the file-format-conversion section 8, the image data read from the image memory 6 is sent to the filing Management Department 13, and file management is carried out.

[0024] Moreover, when digital-watermarking mode is chosen, after image data is inputted into the

digital-watermarking creation section 30 from the file-format-conversion section 8 and digital-watermarking data are embedded at the image data concerned; it is again returned to the file-format-conversion section 8, conversion of a format is performed in it, and file management is carried out to it at the filing Management Department 13.

[0025] Moreover, when alteration prevention mode is chosen, after MAC is added to a header by the approach described above with reference to drawing 2, file management is carried out at the filing Management Department 13.

[0026] Moreover, when alteration detection mode is chosen, detection of the existence of the alteration to the image file which it was acquired from the external device through the storage 17 or the communication line 16 (PC, alteration test equipment, etc.), and was sent to the filing Management Department 13 is performed. That is, the image data to which MAC was added is divided into MAC and image data, image data is inputted into MD creation section 33 from the filing Management Department, and MAC is inputted into the decryption section 34. In MD creation section 33, MD is generated using predetermined functions, such as a Hash Function, from the inputted image data. Moreover, the decryption section 34 generates MD' using the public key Kpublic (camera) memorized by the public key memory 35. It judges whether the comparison coincidence section 32 compares MD and MD', and is in agreement. When both are not in agreement, it turns out that image data was altered by the 3rd person.

[0027] Moreover, secure mode is used when memorizing image data to a storage. In this case, image data is read from the filing Management Department 13, and it is inputted into the encryption section 36. The encryption section 36 enciphers this image data using the share key memorized by the share key memory 37, and sends the enciphered image data to the filing Management Department 13 again. Then, this enciphered image data demounts by control of the record-medium control section 15, and it is written in the possible storage 17.

[0028] Moreover, secure mode is used also when transmitting an image file through a communication line. In this case, image data is read from the filing Management Department 13, and it is inputted into the encryption section 36. The encryption section 36 enciphers this image data using the share key memorized by the share key memory 37, and transmits the enciphered image data to external devices (PC, alteration test equipment, etc.) through a communication line 16 by control of the communications control section 14.

[0029] According to the above-mentioned 2nd operation gestalt, copyright can be kept by taking a photograph by normal mode, when photographing a snap image, and taking a photograph in digital-watermarking mode to alteration supervision mode and the image which wants to keep copyright, for example, in photoing the thing used as an image of evidence. Furthermore, preservation and transmission of data can be carried out to insurance by choosing secure mode to photo the high image of confidentiality and transmit an image file to insurance. Moreover, it becomes possible by combining two or more modes to use one camera for various applications from the above-mentioned effectiveness.

[0030] With reference to drawing 4, the 3rd operation gestalt of this invention is explained below. In drawing 4, the thing of the same reference figure as drawing 1 shall have the same function. Moreover, although the configuration in the communication facility of drawing 1 and the various modes of drawing 3 is omitted here, of course, you may have these functions. In the digital camera 103 of evidence which has the camera section 50-3, the image data obtained by picturizing a photographic subject with the image pick-up means 60 is memorized in an image memory 6. Image data is read from an image memory 6 to the file-format-conversion section 8, and it is changed into the graphics format of criteria, such as JPEG and TIFF. Thereby, the file format by which the data of header information were added to image data is created ((A) of drawing 5).

[0031] The information for personal authentication is read from IC card 40 for personal authentication with which the camera section 50-3 was equipped by control of the IC card control section 41 to coincidence, and it is inputted into the file-format-conversion section 8, and it is recorded as the information for personal authentication shows a header at (B) of drawing 5. Next, in MD creation

section 9, MD is created by applying predetermined functions, such as a Hash Function, to the whole data or image data, and the data for personal authentication ((C) of drawing 5). Next, in the MAC creation section 11, MAC is created by enciphering MD using the private key Kprivate (camera) memorized beforehand in the private key memory 10 ((D) of drawing 5). In addition to the data and the data for personal authentication of image header information, at the header Records Department 12, MAC is stored in an image header. Thereby, in a graphics format as shown in (E) of drawing 5 , an image file is saved at the filing Management Department 13, and file management is carried out.

[0032] Such an image file demounts by control of the storage control section 15, and in order to detect whether it was altered while being memorized and carried by the possible storage 17, alteration detection equipment 104 is used.

[0033] That is, the image file memorized by the storage 17 with which alteration test equipment 104 was equipped is read to the filing Management Department 19 by control of the storage control section 18. At the filing Management Department 19, it separates into the whole data which need an image file to calculate MAC and the above mentioned MAC, i.e., the data except MAC, image data (header information other than the image data itself, such as JPEG and TIFF, may be included in this image data), and the data for personal authentication, MAC is inputted into the decryption section 21, and data required to calculate MAC are inputted into MD creation section 22. Furthermore, the data for personal authentication are inputted also into the individual humanity news read-out section 22.

[0034] In the decryption section 21, MD1 is generated by decrypting MAC using the public key Kpublic (camera) memorized beforehand in the public key memory 20. On the other hand, in MD creation section 22, MD2 is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23, when MD1 is compared with MD2 and both are not in agreement, it can judge with having been altered by the 3rd person.

[0035] Moreover, in the individual humanity news read-out section 42, specification of a photography person is performed by reading the data for personal authentication. Here, specification of a photography person is meaningful only when it is checked that image data is not altered.

[0036] According to the above-mentioned 3rd operation gestalt, not only the existence of an alteration of an image but an image photography person can specify by adding the information for personal authentication at the time of the data origination for alteration detection of image data. Especially, as information for a photography person's personal authentication, since the data for alteration detection are created from the data with which image data and the data for personal authentication were aligned using said encryption key, the alteration of image data and the alteration of a photography person's data for personal authentication are detectable with one alteration detection data here. If a photography person's data for personal authentication are not altered, a photography person can be specified from the data for personal authentication.

[0037] The 4th operation gestalt of this invention is explained below. In drawing 6 , the thing of the same reference figure as drawing 1 shall have the same function. Moreover, although the configuration in the communication facility of drawing 1 and the various modes of drawing 3 is omitted here, of course, you may have these functions. In the digital of-evidence camera system 105 which has the camera section 50-4, the image data obtained by picturizing a photographic subject with the image pick-up means 60 is memorized in an image memory 6. Image data is read from an image memory 6 to the file-format-conversion section 8, and it is changed into the graphics format of criteria, such as JPEG and TIFF. Thereby, the file format by which the data of header information were added to image data is created ((A) of drawing 7). Next, in MD creation section 9, MD1 or MD2 (B [of drawing 7 / (B)], (B)') is generated using predetermined functions, such as a Hash Function, from the whole data or image data. These MD1 and MD2 may be the same. MD1 is inputted into the MAC creation section 11. In the MAC creation section 11, MAC is calculated using the private key Kprivate (camera) beforehand memorized by the private key memory 10, and MAC1 is created ((C) of drawing 7). This MAC1 is sent to the header Records Department 12.

[0038] On the other hand, MD2 is inputted into IC card 40' for personal authentication with which the camera section 50-4 was equipped through the IC card control section 41. In IC card 40' for personal authentication, MD2 is enciphered using the private key Kprivate (IC card) memorized by internal private key memory, and MAC2 is created ((C)' of drawing 7). This MAC2 is sent to the header Records Department 12 through the IC card control section 41.

[0039] In addition to the data of image header information, at the header Records Department 12, MAC1 and MAC2 are stored in an image header. Thereby, in a graphics format as shown in (D) of drawing 7 , an image file is saved at the filing Management Department 13, and file management is carried out.

[0040] Such an image file demounts by control of the storage control section 15, and in order to detect whether it was altered while being memorized and carried by the possible storage 17, alteration detection equipment 106 is used.

[0041] That is, the image file memorized by the storage 17 with which alteration test equipment 106 was equipped is read to the filing Management Department 19 by control of the storage control section 18.

[0042] At the filing Management Department 19, an image file is divided into MAC1, MAC2, and image data (header information other than the image data itself, such as JPEG and TIFF, may be included in this image data), MAC1 is inputted into the decryption section 21-1, and image data is inputted into MD creation section 22-1. In the decryption section 21-1, MD1 is generated by decrypting MAC1 using the public key Kpublic (camera) beforehand memorized by public key memory 20'. A public key Kpublic (camera) and a private key Kprivate (camera) are keys which serve as a pair in encryption/decryption processing. On the other hand, in MD creation section 22-1, MD1' is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23-1, when MD1 is compared with MD1' and both are not in agreement, it can judge with being altered by the 3rd person.

[0043] Similarly, MAC2 is inputted into the decryption section 21-2, and image data is inputted into MD creation section 22-2. In the decryption section 21-2, MD2 is generated by decrypting MAC2 using the public key Kpublic (IC card) beforehand memorized by public key memory 20'. A public key Kpublic (IC card) and a private key Kprivate (IC card) are keys which serve as a pair in encryption/decryption processing.

[0044] On the other hand, in MD creation section 22-2, MD2' is generated using predetermined functions, such as a Hash Function, from the inputted image data. Next, in the comparison coincidence section 23-2, when MD2 is compared with MD2' and both are in agreement, a photography person can be specified.

[0045] According to the above-mentioned 4th operation gestalt, not only the existence of an alteration of an image but an image photography person can specify by adding the information for personal authentication at the time of the data origination for alteration detection of image data. It is possible to apply especially, the electronic signature used with other information systems, such as an electronic mail and electronic commerce, as 2nd data for alteration detection, since the 2nd data for alteration detection created with the equipment of the camera exterior as information for a photography person's personal authentication here is used. Therefore, an infrastructure-[an electronic authentication office, electronic commerce, etc.] information system and the digital of-evidence camera system which was able to take cooperation can also be built.

[0046] Below, the 5th operation gestalt of this invention is explained. The 5th operation gestalt is related with the digital image edit system using the image server constituted from hardware, such as a board and a PCMCIA card. Here, in order to simplify explanation, the minimum configuration of an image server is assumed.

[0047] Conventionally, by the approach using the data for alteration detection used to document data, it was considered that it was altered when original data were changed, even when it was only small. However, about image data, processing of compression, a clipping, insertion of a caption, etc., etc. is needed on the property of data in many cases. If it is the case of the photograph using a film, only a

required part can be burned on printing paper, or it is equivalent to describing a comment on the reverse side of a photograph. If there is a legal excuse, such processing will not be in charge of an alteration. There is the approach of what kind of processing was performed to original image data and recording the processing hysteresis as an approach for judging whether just processing was made.

[0048] With this operation gestalt, it detects whether it is altered with the hysteresis of the performed processing except the image server by using an image server in the image which processed the clipping of a field of compression of a part of image data, the addition of a caption, etc.

[0049] Drawing 8 consists of a personal computer 107-1 and an image server 107-2 which consists of a PCMCIA card with which this personal computer 107-1 can be equipped, as it is drawing showing the configuration of the image server system 107 of the 5th operation gestalt, for example, is shown in drawing 11.

[0050] An operation of the 5th operation gestalt is explained with reference to the flow chart of drawing 9 below. First, the filing Management Department 72 acquires the image file of a format as shown in (A) of drawing 9 from a storage 70 by control of the storage control section 71. Or the image file concerned is acquired from an external device 93 by control of the communications control section 78 through a communication line 77 (step S1). In this case, an image file can be easily inputted from an external device by preparing the filing Management Department 72 connection terminals, such as a serial cable in which direct continuation is possible, and SCSI, IrDA. Moreover, the same effectiveness is acquired even when it has the terminal of network connections, such as Ethernet. Next, the MAC verification section 73 receives an image file from the filing Management Department 72, and verifies MAC1 (step S2). That is, the filing Management Department 72 divides an image file into MAC1 and image data, MAC1 is inputted into the decryption section 75, and image data is inputted into MD creation section 76. The decryption section 75 is decrypted using the public key Kpublic (camera) memorized by the public key memory 74, and creates MD1. Moreover, MD creation section 76 creates MD1' using predetermined functions, such as a Hash Function. By comparing MD1 with MD1', the comparison coincidence section 79 sends the verification result about whether the image photoed with the camera is altered after that to the filing Management Department 72.

[0051] When not altered, an image file is inputted into the image editorial department 93 from the filing Management Department 72, and image edit by the user using the image edit tool 80 is performed (step S3). In this case, the contents of the image file are displayed on an image display device 82, looking at this screen, using data entry units (a keyboard, mouse, etc.) 84, various kinds of processings are required or a user 91 inputs data. 83 is the user interface of a user 91 and the image server 107. The hysteresis at the time of edit is recorded on the edit hysteresis Records Department 81. The edit hysteresis Records Department 81 reads the information for personal authentication from IC card 92 for personal authentication to coincidence by control of the IC card control section 85, and records on it into edit hysteresis. The above-mentioned edit is continued until directions of an edit halt are issued by the user and decision of step S5 serves as NO.

[0052] Since the image file after edit and the data of edit hysteresis are sent to the filing Management Department 72, the filing Management Department 72 records on an image header in a format as shows the information on edit hysteresis to (B) of drawing 9 (step S6). In leaving the information which specifies the photoed camera, it also records camera information on an image header in a format as shown in (C) of drawing 9.

[0053] Next, the image file after edit and the data of edit hysteresis are inputted into MD creation section 87 of the renewal section 86 of an image file from the filing Management Department 72, and MD2 is created using predetermined functions, such as a Hash Function. Next, the MAC creation section 88 creates MAC2 by enciphering MD2 using the private key Kprivate of the image server 107 memorized beforehand (image server) in the private key memory 90 (step S7). At the header Records Department 89, it records on an image header in a format as shows this MAC2 by (D) of drawing 9 (step S8). In leaving the information which specifies a camera, it becomes a format as shown in (E) of drawing

9. The image file to which MAC2 was added is sent to the filing Management Department 72, and after this, it demounts by control of the storage control section 71, and is saved at the possible storage 70, or this image file is sent to an external device 93 through a communication line 77 by control of the communications control section 78, and is saved.

[0054] Since it can check whether what kind of processing was performed from the original image file, or the contents of an image have been changed except an image server by using an image server according to the above-mentioned 5th operation gestalt, it is not altered even if it performs required processing on the property of a data compression or image data like field logging. Moreover, when creating the data for alteration detection added to an image file after edit by the image server, the user who edited the image can be specified by using the data for personal authentication.

[0055] Below, the 6th operation gestalt of this invention is explained. The 6th operation gestalt constitutes the image server in the 5th operation gestalt from software started on PC etc. Here, in order to simplify explanation, the minimum configuration of an image server is assumed.

[0056] Drawing 10 is drawing showing the configuration of the image server system 108 constituted by installing an image server in PC. Here, only a different point from the configuration of the 5th operation gestalt shown in drawing 8 is explained.

[0057] As the 6th operation gestalt shows to drawing 10, it is [the MAC creation section 88 and] a private key Kprivate. The memorized private key memory 90 is formed in the interior of IC card 109 which can be detached and attached freely to the not the interior but image server 108 of the image server system 108. Moreover, the IC card control section 85 is formed in the interior of renewal section of image file 86' of the image server system 108.

[0058] The image file after edit and the data of edit hysteresis are inputted into MD creation section 87 of renewal section of image file 86', and MD2 is created using predetermined functions, such as a Hash Function. This MD2 is sent to the MAC creation section 88 of IC card 109 by control of the IC card control section 85. The MAC creation section 88 enciphers MD2 using a private key Kprivate (IC card), and creates MAC2. This MAC2 is recorded on an image header in a format as sent to the header Records Department 89 by control of the IC card control section 85 and shown in (D) of drawing 9, or (E). In addition, the information for personal authentication is stored in IC card 109 like the 5th operation gestalt, and this is read and you may make it record into edit hysteresis.

[0059] Since according to the above-mentioned 6th operation gestalt in addition to the effectiveness of the 5th operation gestalt it constitutes from a storage in which attachment and detachment like an IC card of management of an encryption key and processing of encryption are free and other functions, such as edit of an image and creation of edit historical data, were constituted from software, it has the effectiveness that an image server can be built by low cost.

[0060] The 7th operation gestalt of this invention is explained below. The 7th operation gestalt consists of a public key server style and a public key acquisition / registration device of alteration test equipment and an image server about decryption key acquisition / registration system. For the private key as encryption and the public key as a decryption key which are used with this operation gestalt, as shown in drawing 13 (A), it is generated by the manufacturer according to the key generation device 120 at the time of manufacture of equipments, such as a digital camera 220, and the image server 221, IC card 222, among these a private key is built-in to equipment, It is registered. This private key is immediately eliminated by insurance and the positive approach after registration.

[0061] Moreover, a public key is memorized by the record medium 203 by the key registration section 202 of the public key server style 110 which equipment is made to correspond with the serial number as an identifier of a proper, and is shown in drawing 13 (B).

[0062] When performing alteration detection to alteration detection equipment and the image by which public key acquisition / registration device 111 of an image server was photoed with the digital camera 220, the serial number of equipment is transmitted to the key retrieval section 204 through the communications control section 211, communication lines 210 and 209, and the communications control

section 208 from the public key acquisition section 212. The key retrieval section 204 reads the public key corresponding to the serial number of equipment from a storage 203, and sends it to MD creation section 205. MD creation section 205 creates MD using predetermined functions, such as a Hash Function, and sends it to the MAC creation section 206. The MAC creation section 206 creates MAC using the private key beforehand memorized by the private key memory 207, and sends it to the public key acquisition section 212 through the communications control section 208, a communication line 209, a communication line 210, and the communications control section 211 with a public key. The public key acquisition section 212 sends the acquired public key and the serial number of equipment to the public key registration section 214. The public key registration section 214 registers a public key and the serial number of equipment concerned into the public key memory 213.

[0063] The data of a public key are sent to MD creation section 216 from the public key acquisition section 212, and MAC is sent to coincidence at the decryption section 217. MD creation section 216 creates MD from the data of this public key using predetermined functions, such as a Hash Function. The decryption section 217 creates MD' by decrypting MAC using the public key Kpublic of the key management server memorized by the public key memory 218 (key management server). The comparison coincidence section 215 detects an alteration by whether MD and MD' is compared and it is in agreement. It is the purpose that by which the camera obtained by means of communications and the public key of an image server were acquired from the just key management server, and that verification of MAC here checks whether it is further altered in the middle of the communication link.

[0064] In addition, you may make it send the public key registered into the public key server 110 to a user with safe means, such as mailing. According to the above-mentioned 7th operation gestalt, the decryption key of the data for alteration detection is acquirable by sending the serial number of equipment to a decryption key (public key) server. When it follows, for example, a decryption key server can be used from the Internet, the data for alteration detection can be acquired even from where among the world based on the serial number of a camera.

[0065] The 8th operation gestalt of this invention is explained below. The 8th operation gestalt is related with alteration prevention of a multiplex resolution image. When a document file changes a part, a text stops connecting, semantics will change and the contents will differ from the original file. Since redundancy of image data is high, even if it performs edit of some, such as modification of resolution, to it, a photographic subject can be recognized in many cases. Therefore, since being the magnitude beyond the need and wanting to drop resolution on the image size at the time of photography and an unnecessary part are reflected, in some cases, I want to start only a required part in the side using an image. However, the image server for alteration prevention must usually be prepared, an image must be edited in the interior, and MAC must be added again.

[0066] So, in the 8th operation gestalt, in order to solve the above-mentioned problem, the image of an alteration prevention camera is saved in the format holding a multiplex resolution image. Drawing 1414 is drawing showing the configuration of the 8th operation gestalt of this invention. In the digital of-evidence camera section 112, the image data obtained by picturizing a photographic subject with the image pick-up means 60 is memorized in an image memory 6. Next, this image data is inputted into the image contraction section 300, and is changed into the image of two or more kinds of resolution. If the minimum resolution to which a user wants to guarantee an alteration through the MAC creation resolution directions section 302 is specified at this time, this will be sent to MD creation section 9 through the filing Management Department 13. In MD creation section 9, MD is created using predetermined functions, such as a Hash Function.

[0067] On the other hand, the private key created from the data of the camera proper memorized by the data memory 301 of a camera proper and the information for personal authentication read from IC card 40 for personal authentication by control of the IC card control section 41 is memorized by the private key memory 10. In the MAC creation section 11, MD created in MD creation section 9 using this private key is enciphered, MAC is created, and it sends to the filing Management Department 13. The filing

Management Department 13 gathers the image data of two or more kinds of resolution in one file, adds MAC created from the data of resolution with which the above was specified further to the image data concerned, and saves by control of the storage control section 15 at a storage 17.

[0068] Drawing 16 is drawing for explaining the image data file of this operation gestalt. As shown in drawing 16, the conversion to a low resolution from high resolution is specified beforehand. MAC is created from the data of the resolution which guarantees the alteration prevention directed in the MAC creation resolution directions section 302, and it records on the header or another MAC management file of image data.

[0069] On the other hand, in alteration test equipment 113, MAC and image data are read from a storage 17 by control of the storage control section 18, and it sends to the filing Management Department 19. At the filing Management Department 9, MAC is sent to the decryption section 21 and image data is sent to an image memory 303. In the decryption section 21, MD1 is created by decrypting MAC using a public key. Moreover, after the image data memorized in the image memory 303 is reduced by the contraction approach predetermined in the image contraction section 304, it is sent to MD creation section 22, and MD2 is created using predetermined functions, such as a Hash Function. In the coincidence comparator 23, it judges whether image data was altered by comparing MD1 with MD2.

[0070] With reference to drawing 15, the 9th operation gestalt of this invention is explained below. The 9th operation gestalt holds the image of multiplex resolution, and the image of each resolution has the intention of preventing the alteration of the graphics format in which the small block of fixed size is stored as a unit. The reason for storing the small block as a unit in this graphics format is because some images can be referred to at a high speed.

[0071] Although the operation of the digital camera 114 of evidence is the same as an operation of the above-mentioned digital camera 112 of evidence, while having image contraction / division section 305 and creating the image of two or more resolution here, as shown in drawing 17, with this operation gestalt, an image is divided per block of fixed magnitude. At the filing Management Department 13, MAC is created for every smallness block and MAC is written in the header for every small block. The image file with MAC is memorized by the storage 17 as an original image by control of the record-medium control section 15.

[0072] The user whose whole photographic coverage and resolution of an image are unnecessary creates logging of a required part and the image of required resolution from the original image read from the storage 17 within common PC115 using the edit software 306 at the time of photography. A user inputs into the image editorial department 306 by making the location of a required image part, size, resolution, etc. into the edit parameter 307. At the filing Management Department 13, the corresponding image block of a location is extracted from the corresponding image of resolution, and it saves at another image file.

[0073] When inspecting an alteration with alteration detection equipment 116, an edited image is read from a storage 17 to the filing Management Department 19 by control of the storage control section 18. In the alteration detection section 308, alteration detection is performed to an edited image. If MAC added for every small block from the first is added to a file new as it is at this time, even if it will not prepare an alteration prevention image server, a user can perform an editing task called modification of field logging of an image or resolution, giving proof nature to an image. Moreover, if it adds the data which recorded the procedure of filtering, without changing the pixel value itself in performing filtering, such as contrast stretching and smoothing, the guarantee of an original image will be attained also about a filtering image.

[0074] In addition, invention of the following configurations is included in the above-mentioned concrete operation gestalt.

1. Image Pick-up Section for being Digital of-Evidence Camera System Which Detects Alteration of Image Data Which Picturized Photographic Subject with Camera and was Obtained, and Picturizing Photographic Subject, The cipher-processing section which creates the data for alteration detection

from the image data obtained by the image pick-up using the encryption key built in beforehand, the camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption -- since -- the digital of-evidence camera system characterized by becoming.

(The operation effectiveness) According to this invention, it can check whether image data is altered by creating the data for alteration detection using the encryption key in a camera from image data, and decrypting this data for alteration detection using the decryption key corresponding to said encryption key. The weight of the evidence of the digital image it was presupposed that it was inferior of a digital image by this compared with the image conventionally photoed using the film can be heightened.

[0075] Moreover, by this invention, although the encryption key for creating the data for alteration detection is not revealed outside by any means including a camera user, since the encryption key for creating the data for alteration detection is beforehand stored in the camera, it can manage an encryption key on very [in hard] high security level.

2. Said cipher-processing section is the digital of-evidence camera system of the configuration 1 publication characterized by creating said data for alteration detection by enciphering the data obtained by said image data with the application of the predetermined function using said encryption key.

(The operation effectiveness) At least, for change, extent of the alteration to image data is a predetermined function (for example, Hash Function) so that it may appear greatly. Since the data for alteration detection were created by enciphering to the data applied and obtained, the data for alteration detection which can ensure alteration detection can be offered.

3. Said alteration detection section is the digital of-evidence camera system of the configuration 2 publication characterized by detecting whether said image data was altered by comparing the data obtained by said image data with the application of said predetermined function with the data which decrypted said data for alteration detection using said decode key, and were obtained.

(The operation effectiveness) Since said data for alteration detection are used, alteration detection can be ensured.

4. Said cipher-processing section is the digital of-evidence camera system of the configuration 1 publication characterized by creating said data for alteration detection based on said encryption key and the data for personal authentication.

(The operation effectiveness) Not only the existence of an alteration of an image but an image photography person can specify by adding the information for personal authentication at the time of the data origination for alteration detection of image data.

5. Said cipher-processing section is the digital of-evidence camera system of the configuration 4 publication characterized by creating the 1st data for alteration detection using said encryption key, creating the 2nd data for alteration detection using said data for personal authentication, setting said 1st and 2nd data for alteration detection from said image data, and considering as said data for alteration detection from said image data.

(The operation effectiveness) Since it uses as data for alteration detection in accordance with the 1st data for alteration detection created from image data, and the 2nd data for alteration detection created from a photography person's data for personal authentication It is possible to apply said 2nd data for alteration detection like the electronic signature used with other information systems, such as an electronic mail and electronic commerce. An infrastructure-[an electronic authentication office, electronic commerce, etc.] information system and the digital of-evidence camera system which was able to take cooperation can also be built.

6. Digital of-evidence camera system of configuration 4 publication characterized by having had the storage section which memorizes said data for personal authentication, and said encryption key, and the 2nd cipher-processing section which creates the 2nd data for alteration detection from said data for personal authentication, and constituting said this 2nd cipher-processing section free [attachment and

detachment] to said camera.

(the operation effectiveness) they be the media (IC card etc.) which can be detach and attach freely to a camera about the 2nd cipher processing section which memorize the data for personal authentication , and an encryption key , and create the 2nd data for alteration detection . by having prepare , even when carrying this medium and the camera of others who do not use usually be use , the existence of an alteration of the image which the individual attested and photoed certainly can be check .

7. Said cipher-processing section is the digital of-evidence camera system of the configuration 4 publication characterized by creating said data for alteration detection using said encryption key from the data with which said image data and said data for personal authentication were aligned.

(The operation effectiveness) In the case of the approach of creating the data for alteration detection using said encryption key, as information for a photography person's personal authentication, the alteration of image data and the alteration of a photography person's data for personal authentication are detectable with one alteration detection data from the data with which image data and the data for personal authentication were aligned. If a photography person's data for personal authentication are not altered, a photography person can be specified from the data for personal authentication.

8. Image Pick-up Section for being Digital of-Evidence Camera System Which Detects Alteration of Image Data Which Picturized Photographic Subject with Camera and was Obtained, and Picturizing Photographic Subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pick-up using the encryption key built in beforehand, The camera to provide and the alteration detection section which detects whether said data for alteration detection were decrypted using the decryption key corresponding to said encryption key, and said image data was altered based on the result of this decryption, since -- the alteration supervision mode as which, as for said camera, said image data detects whether it was altered or not -- in addition, with the secure mode in which encryption to the image data transmitted to said alteration detection section from said camera is performed It has the digital-watermarking mode which embeds digital-watermarking data at image data, and the normal mode which performs the usual photography without using a security function. The digital of-evidence camera system characterized by having the mode selection section for choosing the mode of at least one request from these modes.

(The operation effectiveness) By equipping a camera with the optional feature in various modes, the function of the request according to the purpose of using a camera can be set up. For example, when photographing a snap image, taking a photograph by normal mode and photoing the thing used as an image of evidence, copyright can be kept by taking a photograph in digital-watermarking mode to alteration supervision mode and the image which wants to keep copyright. Furthermore, preservation and transmission of data can be carried out to insurance by choosing secure mode to photo the high image of confidentiality and transmit an image file to insurance. Moreover, it becomes possible by combining two or more modes to use one camera for various applications from the above-mentioned effectiveness.

9. Decryption Key Storage Section Memorized in accordance with 1st Decryption Key corresponding to 1st Encryption Key Generated by Equipment corresponding to Identifier of Proper, and this Identifier, The decryption key output section which creates the data for alteration detection about said 1st decryption key using the 2nd encryption key, and is outputted in accordance with this data for alteration detection, and said 1st decryption key, A preparation ***** server and the decryption key storage section which memorizes said 1st decryption key acquired from said decryption key server through means of communications etc., Said data for alteration detection supplied from said decryption key server through means of communications etc. are decrypted using the 2nd decryption key corresponding to said 2nd encryption key. the decryption key acquisition section equipped with the alteration detection section which detects whether said 1st decryption key was altered based on the result of this decryption -- since -- decryption key acquisition - characterized by becoming Registration system.

(The operation effectiveness) According to this invention, the decryption key of the data for alteration detection is acquirable by sending the serial number of equipment to a decryption key server. When it follows, for example, a decryption key server can be used from the Internet, the data for alteration detection can be acquired even from where among the world based on the serial number of a camera.

10. With Filing Management Department Which is Digital Image Edit System into which Image Data is Edited, and Does Filing Management of the Image Data Inputted through Image Input Section while Detecting Alteration of Image Data While decrypting the 1st data for alteration detection beforehand given to said image data using the decryption key corresponding to the encryption key used when creating this data for alteration detection The alteration detection section which detects the alteration condition of image data by comparing this the 1st decoded data for alteration detection and said image data, To said image data from the edited image data to which various image processings were performed by the image editorial department which performs various kinds of image processings, and said image editorial department, and the data of the edit hysteresis by said image editorial department the renewal section of an image file which creates the 2nd data for alteration detection using an encryption key other than said encryption key, and adds this to said edited image data -- since -- the digital image edit system characterized by becoming.

(The operation effectiveness) According to this invention, since the data for alteration detection are created in accordance with image data and edit hysteresis, it can check what kind of edit processing has been performed to the original image, and can detect further whether image edit processing is performed except the system concerned.

11. Said renewal section of an image file is the digital image edit system of the configuration 10 publication characterized by using said another encryption key for said personal authentication information, and creating said 2nd data for alteration detection while being able to detach and attach freely to a digital image edit system and memorizing said personal authentication information and said another encryption key.

(The operation effectiveness) An image server can be built by low cost with constituting other functions, such as edit of an image and creation of edit historical data, from a storage in which attachment and detachment like an IC card of management of an encryption key and processing of encryption are free by software.

12. The digital image edit system of the configuration 9 publication characterized by uniting and recording personal authentication information on said edit hysteresis.

(The operation effectiveness) The person who edited the image can be specified by including the information for personal authentication in image data also including the data of image edit hysteresis.

13. Said image input section is the digital image edit system of the configuration 9 publication characterized by inputting the image data memorized by external storage by connecting with said image filing section through direct continuation (a cable, IrDA) or a communication line.

(The operation effectiveness) An image file can be easily inputted from an external device by equipping the image filing section of an image server with the terminal of direct continuation, such as a serial cable, and SCSI, IrDA, and the terminal of network connections, such as Ethernet.

14. It is a digital of-evidence camera system the configuration 1 characterized by for said image data be multiplex resolution image data which made the group two or more image data different mutually [resolution] , and memorized it , and said cipher-processing section have the selection section which chooses at least one image data which has desired resolution out of said multiplex resolution image data in order to create said data for alteration detection , or given in ten .

(The operation effectiveness) By specifying the resolution which guarantees alteration detection at the time of record, the user using an image becomes possible [using a desired resolution image without being dependent on the resolution at the time of photography] .

15. it be a digital of evidence camera system the configuration 1 which said image data be a multiplex resolution image data which made the group two or more image data different mutually [resolution] ,

and memorized them , and each image data in said multiplex resolution image data be memorize considering the predetermined small block as a unit , and said cipher processing section be said small block unit , and be characterize by create said data for alteration detection , or given in ten .
(The operation effectiveness) Alteration detection can be carried out also to the image which performed image edit like a clipping, without preparing the server of dedication by adding alteration detection data for every small block.

[0076]

[Effect of the Invention] According to this invention, the weight of the evidence of a digital image can be heightened, the digital of-evidence camera system and decryption key acquisition / registration system which can manage an encryption key on very high security level can be offered, and even if it edits further compression which is needed on the property of an image, field logging, insertion of a caption, etc., the digital image edit system which can maintain the weight of the evidence of a digital image can be offered.

[Translation done.]

*** NOTICES ***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the digital of-evidence camera structure of a system concerning the 1st operation gestalt of this invention.

[Drawing 2] It is drawing showing a procedure until MAC is added to image data.

[Drawing 3] It is drawing showing the configuration of the digital camera of evidence concerning the 2nd operation gestalt of this invention.

[Drawing 4] It is drawing showing the digital of-evidence camera structure of a system concerning the 3rd operation gestalt of this invention.

[Drawing 5] It is drawing showing a procedure until the data for personal authentication and MAC are added to image data.

[Drawing 6] It is drawing showing the digital of-evidence camera structure of a system concerning the 4th operation gestalt of this invention.

[Drawing 7] It is drawing showing a procedure until MAC1 and MAC2 are added to image data.

[Drawing 8] It is drawing showing the image server structure of a system concerning the 5th operation gestalt of this invention.

[Drawing 9] It is a flow chart for explaining an operation of the 5th operation gestalt.

[Drawing 10] It is drawing showing the image server structure of a system concerning the 6th operation gestalt of this invention.

[Drawing 11] It is drawing showing the example of the image server structure of a system of the 5th operation gestalt.

[Drawing 12] It is drawing showing the example of the image server structure of a system of the 6th operation gestalt.

[Drawing 13] It is drawing showing decryption key acquisition / registration structure of a system concerning the 7th operation gestalt of this invention.

[Drawing 14] It is drawing showing the digital of-evidence camera structure of a system concerning the 8th operation gestalt of this invention.

[Drawing 15] It is drawing showing the digital of-evidence camera structure of a system concerning the 9th operation gestalt of this invention.

[Drawing 16] It is drawing for explaining the image data file concerning the 8th operation gestalt.

[Drawing 17] It is drawing for explaining the image data file concerning the 9th operation gestalt.

[Description of Notations]

- 1 -- Image pick-up lens,
- 2 -- Image sensor,
- 3 -- Amplifier,
- 4 -- A/D-conversion section,
- 5 -- Signal-processing section,
- 6 -- Image memory
- 7 -- Image display section,
- 8 -- File-format-conversion section,
- 9 -- MD creation section,
- 10 -- Private key memory,
- 11 -- MAC creation section,
- 12 -- Header Records Department,
- 13 -- Filing Management Department,
- 14 -- Communications control section,
- 15 -- Storage control section,
- 16 -- Communication line,
- 17 -- Storage,
- 18 -- Storage control section,
- 19 -- Filing Management Department,
- 20 -- Public key memory,
- 21 -- Decryption section,
- 22 -- MD creation section,
- 23 -- Comparison coincidence section,
- 24 -- Communications control section,
- 25 -- Communication line,
- 50-1 -- Camera section,
- 60 -- Image pick-up means,
- 100 -- Digital camera of evidence,
- 101 -- Alteration test equipment.

[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-308564

(43) 公開日 平成11年(1999)11月5日

(51) Int.Cl.⁵

識別記号

F I

H 0 4 N 5/91

H 0 4 N 5/91

J

G 0 9 C 5/00

G 0 9 C 5/00

H 0 4 N 5/765

H 0 4 N 5/781

5 1 0 J

5/781

5/92

H

5/92

審査請求 未請求 請求項の数 4 O L (全 17 頁)

(21) 出願番号

特願平10-109352

(22) 出願日

平成10年(1998)4月20日

(71) 出願人 000000376

オリンパス光学工業株式会社

東京都渋谷区幡ヶ谷2丁目43番2号

(72) 発明者 近藤 隆

東京都渋谷区幡ヶ谷2丁目43番2号 オリ
ンパス光学工業株式会社内

(72) 発明者 日暮 正樹

東京都渋谷区幡ヶ谷2丁目43番2号 オリ
ンパス光学工業株式会社内

(72) 発明者 小宮 康宏

東京都渋谷区幡ヶ谷2丁目43番2号 オリ
ンパス光学工業株式会社内

(74) 代理人 弁理士 鈴江 武彦 (外4名)

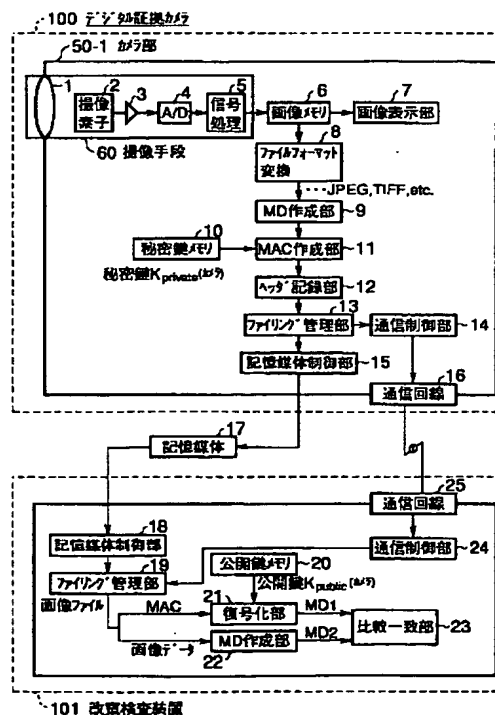
最終頁に続く

(54) 【発明の名称】 デジタル証拠カメラシステム、復号化鍵取得・登録システム、及びデジタル画像編集システム

(57) 【要約】

【課題】デジタル画像の証拠能力を高めて、暗号化鍵を極めて高いセキュリティレベルで管理することができるデジタル証拠カメラシステムを提供する。

【解決手段】カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像手段60と、撮像により得られた画像データから、あらかじめ内蔵された秘密鍵を用いて改竄検知用データ(MAC)を作成するMAC作成部11とを具備するカメラ部50-1と、秘密鍵に対応する公開鍵を用いてMACを復号化し、この復号化の結果に基づいて画像データが改竄されたか否かを検知する改竄検査装置101とからなる。



(2)

【特許請求の範囲】

【請求項 1】 カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、

被写体を撮像するための撮像部と、

撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、

を具備するカメラと、

前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、

からなることを特徴とするデジタル証拠カメラシステム。

【請求項 2】 カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、

被写体を撮像するための撮像部と、

撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、

を具備するカメラと、

前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、

からなり、

前記カメラは、前記画像データが改竄されたか否かを検知する改竄監視モードに加えて、前記カメラから前記改竄検知部へ転送される画像データに対する暗号化を行なうセキュアモードと、電子透かしデータを画像データに埋め込む電子透かしモードと、セキュリティ機能を働かせないで通常の撮影を行なうノーマルモードとを有し、これらのモードから少なくとも 1 つの所望のモードを選択するためのモード選択部を有することを特徴とするデジタル証拠カメラシステム。

【請求項 3】 装置に固有の識別子と、この識別子に対応して生成された第 1 の暗号化鍵に対応する第 1 の復号化鍵とをあわせて記憶する復号化鍵記憶部と、

前記第 1 の復号化鍵に関する改竄検知用データを第 2 の暗号化鍵を用いて作成し、この改竄検知用データと前記第 1 の復号化鍵とをあわせて出力する復号化鍵出力部と、

を備えた復号化鍵サーバと、

前記復号化鍵サーバから通信手段等を介して取得した前記第 1 の復号化鍵を記憶する復号化鍵記憶部と、

前記第 2 の暗号化鍵に対応する第 2 の復号化鍵を用いて、通信手段等を介して前記復号化鍵サーバから供給された前記改竄検知用データを復号化し、この復号化の結

2

果に基づいて前記第 1 の復号化鍵が改竄されたか否かを検知する改竄検知部と、

を備えた復号化鍵取得部と、

からなることを特徴とする復号化鍵取得・登録システム。

【請求項 4】 画像データの改竄を検知するとともに、画像データの編集を行なうデジタル画像編集システムであって、

画像入力部を介して入力された画像データをファイリング管理するファイリング管理部と、

前記画像データにあらかじめ付与された第 1 の改竄検知用データを、この改竄検知用データを作成する際に用いた暗号化鍵に対応する復号化鍵を用いて復号化するとともに、この復号された第 1 の改竄検知用データと前記画像データとを比較することにより画像データの改竄状態を検知する改竄検知部と、

前記画像データに対し、各種の画像処理を施す画像編集部と、

前記画像編集部によって各種画像処理を施された編集済み画像データと前記画像編集部による編集履歴のデータから、前記暗号化鍵とは別の暗号化鍵を用いて第 2 の改竄検知用データを作成し、これを前記編集済み画像データに付加する画像ファイル更新部と、

からなることを特徴とするデジタル画像編集システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデジタル証拠カメラシステム、復号化鍵取得・登録システム、及びデジタル画像編集システムに関する。

【0002】

【従来の技術】従来、例えば、カメラのフィルムやメディアにアナログで記録された写真や音声は、裁判等において証明力のあるものとして用いられている。近年のデジタル技術の進歩により、画像や音声をデジタルデータとして記録する装置が普及している。このようなデジタル化によれば、コピーしても劣化しない、通信回線を使って素早く配布できる、さらに情報内容の加工・編集を容易に行えるという長所が得られる。しかし、加工・編集が容易であるということは、一方で情報内容を容易に改竄できるということであり、情報として証拠能力が疑われる余地が生まれる。したがって、デジタルの画像や音声を証拠品として使えるようにするためには、なんらかの方法でデジタルデータの改竄を防止する機能を備えていることが必要である。このような防止機能を有するカメラはデジタル証拠カメラと呼ばれている。

【0003】このデジタル証拠カメラを実現するために、一般に通信等で用いられている電子署名技術を応用することが考えられている。電子署名システムでは、対となる 2 つの鍵が用いられる。1 つは、暗号化のための鍵で秘密鍵と呼ばれ、もう一方は復号化のための鍵で公

(3)

3

開鍵と呼ばれる。デジタルデータは秘密鍵を用いて暗号化され、公開鍵を用いて復号化される。秘密鍵から公開鍵を求めるには一方向性関数を用いられるが、この一方向性関数の性質により、逆に公開鍵から秘密鍵を求めることは数学的に非常に難しいものとなっている。秘密鍵は持ち主以外の人が絶対に使えないように厳重に管理される必要がある一方、公開鍵は誰でも使えるように一般に公開される。

【0004】改竄検知の方法は、送信側で、まず対象のデジタルデータからハッシュ関数などを使って、メッセージ・ダイジェスト (Message Digest、以下、MD) と呼ばれるコードを作成する。対象のデジタルデータからMDを抽出する方法は公開されており、オリジナルデータがあれば誰でもMDを抽出することはできる。ちなみに、MDはハッシュ関数の良く知られた性質から元のデジタルデータが少しでも異なると値が大きく変化するという性質がある。

【0005】次に抽出されたMDを秘密鍵を用いて暗号化し、これをメッセージ認証子 (Message Authentication Code、以下、MAC) として、オリジナルデータとともに相手側に送信する。ここで、秘密鍵と対となる公開鍵は受信者に確実に渡されているものとする (受信者が必ずその鍵を手にいれていればよく、第3者の手に渡ってもかまわない)。

【0006】受信側は、オリジナルデータが改竄されていないことを調べるために、まず、オリジナルデータからハッシュ関数などを用いてMD' を求める。次に公開鍵を用いてMACを復号化してMDを求め、このMDとMD' とが一致するかどうかを調べる。もし、オリジナルデータが第3者によって改竄されたとしても、第3者は秘密鍵を持っていないので、公開鍵で復号化できるMACを作成できず、MDとMD' とは異なる値となる。これによって、オリジナルデータが第3者によって改竄されたことがわかる。

【0007】

【発明が解決しようとする課題】上記したように、デジタルデータの改竄を検知するために電子署名技術を応用することができる。しかしながら、上記したような改竄検知の方法をデジタル証拠カメラに採用した場合、暗号化鍵としての秘密鍵は絶対漏洩することがあってはならないが、従来はこの秘密鍵を高いセキュリティレベルで管理することが容易でなく、したがって、デジタル画像の証拠能力を高めることができなかった。

【0008】また、画像の場合にはデータの性質上、データ圧縮や領域切り出し、キャプションの挿入等の処理を施す必要のある場合が多いが、従来、文書データに対して応用されている電子署名の方法では、データ内容が僅かでも変更すると、データが改竄されたと見なされてしまう。したがって、従来の電子署名システムでは、上記のような画像データの性質上必要な編集が一切できな

4

かった。

【0009】本発明はこのような課題に着目してなされたものであり、その目的とするところは、デジタル画像の証拠能力を高めることができ、暗号化鍵を極めて高いセキュリティレベルで管理することができるデジタル証拠カメラシステム、復号化鍵取得・登録システムを提供することであり、さらに画像の性質上必要となる圧縮や領域切り出し、キャプションの挿入等の編集を施してもデジタル画像の証拠能力を保てるデジタル画像編集システムを提供することにある。

【0010】

【課題を解決するための手段】上記の目的を達成するために、第1の発明は、カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部とからなる。

【0011】また、第2の発明は、カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部とからなり、前記カメラは、前記画像データが改竄されたか否かを検知する改竄監視モードに加えて、前記カメラから前記改竄検知部へ転送される画像データに対する暗号化を行なうセキュアモードと、電子透かしデータを画像データに埋め込む電子透かしモードと、セキュリティ機能を働かせないで通常の撮影を行なうノーマルモードとを有し、これらのモードから少なくとも1つの所望のモードを選択するためのモード選択部を有する。

【0012】また、第3の発明は、復号化鍵取得・登録システムであって、装置に固有の識別子と、この識別子に対応して生成された第1の暗号化鍵に対応する第1の復号化鍵とをあわせて記憶する復号化鍵記憶部と、前記第1の復号化鍵に関する改竄検知用データを第2の暗号化鍵を用いて作成し、この改竄検知用データと前記第1の復号化鍵とをあわせて出力する復号化鍵出力部と、を備えた復号化鍵サーバと、前記復号化鍵サーバから通信手段等を介して取得した前記第1の復号化鍵を記憶する復号化鍵記憶部と、前記第2の暗号化鍵に対応する第2の復号化鍵を用いて、通信手段等を介して前記復号化鍵サーバから供給された前記改竄検知用データを復号化

(4)

5

し、この復号化の結果に基づいて前記第1の復号化鍵が改竄されたか否かを検知する改竄検知部と、を備えた復号化鍵取得部とからなる。

【0013】また、第4の発明は、画像データの改竄を検知するとともに、画像データの編集を行なうデジタル画像編集システムであって、画像入力部を介して入力された画像データをファイリング管理するファイリング管理部と、前記画像データにあらかじめ付与された第1の改竄検知用データを、この改竄検知用データを作成する際に用いた暗号化鍵に対応する復号化鍵を用いて復号化するとともに、この復号された第1の改竄検知用データと前記画像データとを比較することにより画像データの改竄状態を検知する改竄検知部と、前記画像データに対し、各種の画像処理を施す画像編集部と、前記画像編集部によって各種画像処理を施された編集済み画像データと前記画像編集部による編集履歴のデータから、前記暗号化鍵とは別の暗号化鍵を用いて第2の改竄検知用データを作成し、これを前記編集済み画像データに付加する画像ファイル更新部とからなる。

【0014】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を詳細に説明する。図1は本発明の第1実施形態に係るデジタル証拠カメラシステムの構成を示す図であり、デジタル証拠カメラ100と改竄検査装置101とから構成される。デジタル証拠カメラ100のカメラ部50-1は、撮影レンズ1と、撮像素子2と、増幅器3と、A/D変換器4と、信号処理部5とからなる撮像手段60を有する。撮影レンズ1を介して入射した被写体像は撮像素子2により撮像される。この撮像により得られた電気信号は増幅器3により増幅され、A/D変換部4でデジタル信号に変換されて信号処理部5で所定の信号処理が施された後、画像データとして画像メモリ6に記憶される。この画像メモリ6に記憶されている画像データは必要に応じて画像表示部7に表示される。

【0015】画像メモリ6に記憶されている画像データはファイルフォーマット変換部8において、JPEG、TIFFなどの標準の画像フォーマットに変換される。これにより、画像データにヘッダ情報のデータが付加されたファイルフォーマットが作成される（図2の

(A)）。次にMD作成部9では、画像データあるいはヘッダをも含めた全体のデータに対してハッシュ関数などの所定の関数を適用することによりMDを作成する

（図2の(B)）。次に、MAC作成部11では、秘密鍵メモリ10にあらかじめ記憶された秘密鍵 $K_{private}$ （カメラ）を用いてMDを暗号化することによりMACを作成する（図2の(C)）。次に、ヘッダ記録部11では、作成したMACを画像ヘッダ中に格納する（図2の(D)）。ファイリング管理部13ではこのようにして作成されたファイルフォーマットの画像ファイルに対するファイル管理を行う。

6

【0016】このような画像ファイルが記憶媒体制御部15の制御により取外し可能な記憶媒体17に記憶されて持ち運ばれる間に、あるいは通信制御部14の制御により通信回線16を介して送信される途中で改竄されたか否かを検知するために、改竄検知装置101が用いられる。

【0017】すなわち、改竄検査装置101に装着された記憶媒体17に記憶されている画像ファイルは、記憶媒体制御部18の制御によりファイリング管理部19に読み出される。あるいは、当該画像ファイルは通信制御部24の制御により通信回線25を介してファイリング管理部19へと送られる。ファイリング管理部19では、画像ファイルがMACと画像データ（この画像データには、画像データそのものの他に、JPEGやTIFF等のヘッダ情報を含めてもよい）とに分離され、MACは復号化部21に入力され、画像データはMD作成部22に入力される。

【0018】復号化部21では公開鍵メモリ20にあらかじめ記憶されている公開鍵 K_{public} （カメラ）を用いてMACを復号化することによりMD1を生成する。この公開鍵 K_{public} （カメラ）と前記した秘密鍵 $K_{private}$ （カメラ）とは、暗号化／復号化処理においてペアとなる鍵である。一方、MD作成部22では入力された画像データからハッシュ関数などの所定の関数を用いてMD2を生成する。次に、比較一致部23ではMD1とMD2とを比較して両者が一致しなかった場合には画像ファイルが第三者により改竄されたと判定することができる。

【0019】上記した第1実施形態によれば、画像データからカメラ内の暗号化鍵を用いて改竄検知用データ（MAC）を作成し、この改竄検知用データを画像ファイル内、例えば画像のヘッダ情報内に書き込んでおくことで、画像データが改竄されているかどうかを確認できる。これにより、従来フィルムを用いて撮影された画像に比べ、劣るとされていたデジタル画像の証拠能力を高めることができる。

【0020】また、改竄検知用データを作成するための暗号化鍵は、カメラ利用者を含め外部に絶対に漏洩することがあってはならないが、本実施形態では改竄検知用データを作成するための暗号化鍵は、あらかじめカメラ内のメモリ領域に格納されるため、暗号化鍵をハード的に極めて高いセキュリティレベルで管理できる。

【0021】次に本発明の第2実施形態として、各種のモード（マルチモード）を有するデジタル証拠カメラについて説明する。ここでは、カメラに以下の各種モードの選択機能を備えることで、カメラの使用目的に応じた所望の機能を設定できる。ここで各種モードとは、セキュリティ機能を働かせない通常の撮影モード、撮影した画像ファイルに改竄検知データを付与する改竄監視モード、また、撮影した写真の著作権情報を画像ファイルに

(5)

7

電子透かしとして記録する電子透かしモード、さらには画像ファイルを取り外し可能な記憶媒体に保存する場合、あるいは通信機能を用いて画像ファイルを送信する場合に画像ファイルを暗号化するセキュアモード、等である。

【0022】以下、図3を参照してさらに詳細に説明する。図3において図1と同一の参照番号を有するものは同一の機能を有するものとする。この実施形態におけるカメラ部50-2からなるデジタル証拠カメラ102において、使用者はモード選択部31で上記した各種のモードのうちから所望のモードを選択することができる。

【0023】例えば、ノーマルモードを選択したときには、撮像手段60により被写体を撮像して得られた画像データが画像メモリ6に記憶される。このモードでは特にセキュリティモードは働かず、画像メモリ6から読み出された画像データはファイルフォーマット変換部8でフォーマット変換されてファイリング管理部13に送られてファイル管理される。

【0024】また、電子透かしモードを選択した場合には、画像データがファイルフォーマット変換部8から電子透かし作成部30に入力されて当該画像データに電子透かしデータが埋め込まれた後、ファイルフォーマット変換部8に再び戻されてフォーマットの変換が行われ、ファイリング管理部13でファイル管理される。

【0025】また、改竄防止モードを選択した場合には、図2を参照して前記した方法でヘッダにMACが付加された後、ファイリング管理部13にてファイル管理される。

【0026】また、改竄検知モードが選択された場合には、記憶媒体17あるいは通信回線16を介して外部装置（PC、改竄検査装置など）から取得されてファイリング管理部13に送られた画像ファイルに対する改竄の有無の検知が行われる。すなわち、MACが付加された画像データはMACと画像データとに分離され、画像データはファイリング管理部からMD作成部33に入力され、MACは復号化部34に入力される。MD作成部33では入力された画像データからハッシュ関数などの所定の関数を用いてMDを生成する。また、復号化部34は公開鍵メモリ35に記憶されている公開鍵K_{public}（カメラ）を用いてMD'を生成する。比較一致部32はMDとMD'とを比較して一致するか否かを判断する。両者が一致しなかった場合には画像データが第三者により改竄されたことがわかる。

【0027】また、セキュアモードは画像データを記憶媒体に記憶するときに用いられる。この場合には、ファイリング管理部13から画像データが読み出されて暗号化部36に入力される。暗号化部36はこの画像データを共有鍵メモリ37に記憶されている共有鍵を用いて暗号化し、暗号化した画像データを再度ファイリング管理部13に送る。その後、記録媒体制御部15の制御によ

8

りこの暗号化された画像データが取外し可能な記憶媒体17に書き込まれる。

【0028】また、セキュアモードは通信回線を介して画像ファイルを伝送するときにも用いられる。この場合には、ファイリング管理部13から画像データが読み出されて暗号化部36に入力される。暗号化部36はこの画像データを共有鍵メモリ37に記憶されている共有鍵を用いて暗号化し、暗号化した画像データを通信制御部14の制御により通信回線16を介して外部装置（PC、改竄検査装置など）に送信する。

【0029】上記した第2実施形態によれば、例えば、スナップ画像を撮る時にはノーマルモードで撮影し、証拠画像となるものを撮影する場合には改竄監視モード、また、著作権を守りたい画像に対しては電子透かしモードで撮影することで著作権を守ることができる。さらに、機密性の高い画像を撮影し、画像ファイルを安全に送信したい場合には、セキュアモードを選択することで、データの保存や送信を安全に行うことができる。また、複数のモードを組み合わせることで上記の効果から、1台のカメラを様々な用途に利用することが可能となる。

【0030】以下に図4を参照して本発明の第3実施形態を説明する。図4において、図1と同様の参照数字のものは同様の機能を有するものとする。また、ここでは図1の通信機能及び図3の各種モードの構成を省略しているが、これらの機能を備えていても良いことは勿論である。カメラ部50-3を有するデジタル証拠カメラ103において、撮像手段60によって被写体を撮像することによって得られた画像データは画像メモリ6に記憶される。画像メモリ6から画像データがファイルフォーマット変換部8に読み出されて、JPEG、TIFFなどの標準の画像フォーマットに変換される。これにより、画像データにヘッダ情報のデータが付加されたファイルフォーマットが作成される（図5の（A））。

【0031】同時に、ICカード制御部41の制御によりカメラ部50-3に装着された個人認証用ICカード40から個人認証用の情報が読み出されてファイルフォーマット変換部8に入力されて、ヘッダに個人認証用の情報が図5の（B）に示すように記録される。次にMD作成部9では、データ全体、もしくは画像データ及び個人認証用データに対してハッシュ関数などの所定の関数を適用することによりMDを作成する（図5の（C））。

次に、MAC作成部11では、秘密鍵メモリ10にあらかじめ記憶された秘密鍵K_{private}（カメラ）を用いてMDを暗号化することによりMACを作成する（図5の（D））。ヘッダ記録部12では、画像ヘッダ中に画像ヘッダ情報のデータ及び個人認証用データに加えて、MACを格納する。これにより、画像ファイルは図5の（E）に示すような画像フォーマットでファイリング管理部13に保存されてファイル管理される。

(6)

9

【0032】このような画像ファイルが記憶媒体制御部15の制御により取外し可能な記憶媒体17に記憶されて持ち運ばれる間に改竄されたか否かを検知するために、改竄検知装置104が用いられる。

【0033】すなわち、改竄検査装置104に装着された記憶媒体17に記憶されている画像ファイルは、記憶媒体制御部18の制御によりファイリング管理部19に読み出される。ファイリング管理部19では、画像ファイルがMACと前記したMACを求めるのに必要なデータ、すなわちMACを除くデータ全体、もしくは画像データ（この画像データには、画像データそのものの他に、J P E GやT I F F等のヘッダ情報を含めてもよい）及び個人認証用データ、とに分離され、MACは復号化部21に入力され、MACを求めるのに必要なデータはMD作成部22に入力される。さらに個人認証用データは個人情報読み出し部22にも入力される。

【0034】復号化部21では公開鍵メモリ20にあらかじめ記憶されている公開鍵 K_{public} （カメラ）を用いてMACを復号化することによりMD1を生成する。一方、MD作成部22では入力された画像データからハッシュ関数などの所定の関数を用いてMD2を生成する。次に、比較一致部23ではMD1とMD2とを比較して両者が一致しなかった場合には第3者により改竄されたと判定することができる。

【0035】また、個人情報読み出し部42では個人認証用データを読み出すことにより撮影者の特定が行われる。ここで、撮影者の特定は、画像データが改竄されていないことが確認された場合にのみ意味がある。

【0036】上記した第3実施形態によれば、画像データの改竄検知用データ作成時に、個人認証用の情報も付加することで、画像の改竄の有無のみならず、画像撮影者も特定することができる。特に、ここでは、撮影者の個人認証用の情報として、画像データと個人認証用データを合わせたデータから、前記暗号化鍵を用いて改竄検知用データを作成しているので、1つの改竄検知データで、画像データの改竄と撮影者の個人認証用データの改竄を検知できる。撮影者の個人認証用データが改竄されてなければ、個人認証用データから撮影者を特定できる。

【0037】以下に本発明の第4実施形態を説明する。図6において、図1と同様の参照数字のものは同様の機能を有するものとする。また、ここでは図1の通信機能及び図3の各種モードの構成を省略しているが、これらの機能を備えていても良いことは勿論である。カメラ部50-4を有するデジタル証拠カメラシステム105において、撮像手段60によって被写体を撮像することによって得られた画像データは画像メモリ6に記憶される。画像メモリ6から画像データがファイルフォーマット変換部8に読み出されて、J P E G、T I F Fなどの標準の画像フォーマットに変換される。これにより、画

10

像データにヘッダ情報のデータが付加されたファイルフォーマットが作成される（図7の（A））。次にMD作成部9においてデータ全体、もしくは画像データからハッシュ関数などの所定の関数を用いてMD1あるいはMD2（図7の（B）、（B）'）を生成する。このMD1とMD2とは同一のものであってもよい。MD1はMAC作成部11に入力される。MAC作成部11では秘密鍵メモリ10にあらかじめ記憶されている秘密鍵 $K_{private}$ （カメラ）を用いてMACを計算してMAC1を作成する（図7の（C））。このMAC1はヘッダ記録部12に送られる。

【0038】一方、MD2はICカード制御部41を介して、カメラ部50-4に装着された個人認証用ICカード40'に入力される。個人認証用ICカード40'では、内部の秘密鍵メモリに記憶されている秘密鍵 $K_{private}$ （ICカード）を用いてMD2を暗号化してMAC2を作成する（図7の（C）'）。このMAC2は、ICカード制御部41を介してヘッダ記録部12に送られる。

【0039】ヘッダ記録部12では、画像ヘッダ中に、画像ヘッダ情報のデータに加えて、MAC1とMAC2とを格納する。これにより、画像ファイルは図7の（D）に示すような画像フォーマットでファイリング管理部13に保存されてファイル管理される。

【0040】このような画像ファイルが記憶媒体制御部15の制御により取外し可能な記憶媒体17に記憶されて持ち運ばれる間に改竄されたか否かを検知するために、改竄検知装置106が用いられる。

【0041】すなわち、改竄検査装置106に装着された記憶媒体17に記憶されている画像ファイルは、記憶媒体制御部18の制御によりファイリング管理部19に読み出される。

【0042】ファイリング管理部19では、画像ファイルがMAC1、MAC2と画像データ（この画像データには、画像データそのものの他に、J P E GやT I F F等のヘッダ情報を含めてもよい）とに分離され、MAC1は復号化部21-1に入力され、画像データはMD作成部22-1に入力される。復号化部21-1では公開鍵メモリ20'にあらかじめ記憶されている公開鍵 K_{public} （カメラ）を用いてMAC1を復号化することによりMD1を生成する。公開鍵 K_{public} （カメラ）と秘密鍵 $K_{private}$ （カメラ）とは、暗号化／復号化処理においてペアとなる鍵である。一方、MD作成部22-1では入力された画像データからハッシュ関数などの所定の関数を用いてMD1'を生成する。次に、比較一致部23-1ではMD1とMD1'とを比較して両者が一致しなかった場合には第3者により改竄されていると判定することができる。

【0043】同様にして、MAC2は復号化部21-2に入力され、画像データはMD作成部22-2に入力さ

(7)

11

れる。復号化部21-2では公開鍵メモリ20'にあらかじめ記憶されている公開鍵 K_{public} (ICカード)を用いてMAC2を復号化することによりMD2を生成する。公開鍵 K_{public} (ICカード)と秘密鍵 K_{private} (ICカード)とは、暗号化/復号化処理においてペアとなる鍵である。

【0044】一方、MD作成部22-2では入力された画像データからハッシュ関数などの所定の関数を用いてMD2'を生成する。次に、比較一致部23-2ではMD2とMD2'とを比較して両者が一致したときには撮影者を特定することができる。

【0045】上記した第4実施形態によれば、画像データの改竄検知用データ作成時に、個人認証用の情報も付加することで、画像の改竄の有無のみならず、画像撮影者も特定することができる。特に、ここでは、撮影者の個人認証用の情報として、カメラ外部の装置で作成した第2の改竄検知用データを用いているので、第2の改竄検知用データとして電子メールや電子商取引など他の情報システムで用いられている電子署名を応用することが可能である。したがって、電子公証局や電子商取引などの社会基盤的な情報システムと連携が取れたデジタル証拠カメラシステムを構築することもできる。

【0046】以下に、本発明の第5実施形態を説明する。第5実施形態は例えばボード、PCMCIAカード等のハードウェアにて構成したイメージサーバを用いたデジタル画像編集システムに関するものである。ここでは説明を簡単にするためにイメージサーバの最小限の構成を想定する。

【0047】従来、文書データに対して用いられている改竄検知用データを用いる方法では、オリジナルデータをほんのわずかでも改変すると改竄されたと見なされた。しかし、画像データに関してはデータの性質上、圧縮や切り抜き、キャプションの挿入等の処理が必要になる場合が多い。フィルムを用いた写真の場合であれば、必要な部分だけ印画紙に焼き付けたり、写真の裏にコメントを記述することに相当する。正当な理由があれば、このような処理は改竄にあたらない。正当な処理がなされたかどうかを判断できるようにするための方法としては、オリジナル画像データにどのような処理が施されたのか、その処理履歴を記録する方法がある。

【0048】本実施形態では、イメージサーバを用いることで、画像データの圧縮、一部の領域の切り抜き、キャプションの追加などの処理を施した画像には、施した処理の履歴とともに、イメージサーバ以外で改竄されているかどうかを検知するようにする。

【0049】図8は第5実施形態のイメージサーバシステム107の構成を示す図であり、例えば図11に示すように、パソコン107-1と、このパソコン107-1に装着可能なPCMCIAカードからなるイメージサーバ107-2とから構成される。

12

【0050】以下に第5実施形態の作用を図9のフローチャートを参照して説明する。まず、ファイリング管理部72は、記憶媒体制御部71の制御により記憶媒体70から、図9の(A)に示すようなフォーマットの画像ファイルを取得する。あるいは、外部装置93から通信回線77を介して通信制御部78の制御により当該画像ファイルを取得する(ステップS1)。この場合、ファイリング管理部72に直接接続可能な、シリアルケーブル、SCSI、IrDA等の接続端子を設けておくことで外部装置から容易に画像ファイルを入力することができる。また、イーサネット等のネットワーク接続の端子を備えた場合でも同様の効果が得られる。次に、MAC検証部73は、ファイリング管理部72から画像ファイルを受け取ってMAC1を検証する(ステップS2)。すなわち、ファイリング管理部72は画像ファイルをMAC1と画像データとに分離し、MAC1は復号化部75に入力され、画像データはMD作成部76に入力される。復号化部75は公開鍵メモリ74に記憶された公開鍵 K_{public} (カメラ)を用いて復号化してMD1を作成する。また、MD作成部76はハッシュ関数などの所定の関数を用いてMD1'を作成する。比較一致部79はMD1とMD1'とを比較することにより、カメラで撮影された画像がその後改竄されているか否かに関する検証結果をファイリング管理部72に送る。

【0051】改竄されていない場合には、画像ファイルはファイリング管理部72から画像編集部93に入力されて画像編集ツール80を用いたユーザによる画像編集が行われる(ステップS3)。この場合、画像ファイルの内容は画像表示装置82に表示され、ユーザ91はこの画面を見ながらデータ入力装置(キーボード、マウス等)84を用いて各種の処理の要求を行ったり、データを入力する。83はユーザ91とイメージサーバ107とのユーザインタフェースである。編集時の履歴は編集履歴記録部81に記録される。同時に、編集履歴記録部81は、ICカード制御部85の制御により個人認証用ICカード92から個人認証用の情報を読み出して編集履歴中に記録する。上記編集はユーザから編集停止の指示が出されステップS5の判断がNOとなるまで継続される。

【0052】編集後の画像ファイルと編集履歴のデータはファイリング管理部72に送られるので、ファイリング管理部72は編集履歴の情報を図9の(B)に示すようなフォーマットで画像ヘッダに記録する(ステップS6)。撮影したカメラを特定する情報を残す場合には、図9の(C)に示すようなフォーマットでカメラ情報も画像ヘッダに記録する。

【0053】次に、編集後の画像ファイルと編集履歴のデータとがファイリング管理部72から画像ファイル更新部86のMD作成部87に入力されてハッシュ関数などの所定の関数を用いてMD2が作成される。次に、M

(8)

13

AC作成部88は秘密鍵メモリ90にあらかじめ記憶されているイメージサーバ107の秘密鍵 $K_{private}$ （イメージサーバ）を用いてMD2を暗号化することによりMAC2を作成する（ステップS7）。ヘッダ記録部89ではこのMAC2を図9の（D）で示すようなフォーマットで画像ヘッダに記録する（ステップS8）。カメラを特定する情報を残す場合には図9の（E）に示すようなフォーマットになる。MAC2が付加された画像ファイルはファイリング管理部72に送られ、この後、この画像ファイルは、記憶媒体制御部71の制御により取

10 外し可能な記憶媒体70に保存されるか、あるいは、通信制御部78の制御により通信回線77を介して外部装置93に送られて保存される。

【0054】上記した第5実施形態によれば、イメージサーバを用いることで、オリジナルの画像ファイルからどのような処理が施されたか、また、イメージサーバ以外で画像内容が変更されたかどうかを確認できるため、データ圧縮や領域切り出しのような、画像データの性質上必要な処理を施しても改竄とならない。また、イメージサーバで編集後に画像ファイルに付加する改竄検知用

データを作成するときに、個人認証用データも用いることで、画像を編集したユーザを特定することができる。

【0055】以下に、本発明の第6実施形態を説明する。第6実施形態は第5実施形態におけるイメージサーバをPC等の上で起動されるソフトウェアにて構成したものである。ここでは説明を簡単にするためにイメージサーバの最小限の構成を想定する。

【0056】図10はイメージサーバをPCにインストールして構成されるイメージサーバシステム108の構成を示す図である。ここでは図8に示す第5実施形態の構成と異なる点についてのみ説明する。

【0057】第6実施形態では図10に示すように、MAC作成部88と、秘密鍵 $K_{private}$ が記憶された秘密鍵メモリ90とが、イメージサーバシステム108の内部ではなく、イメージサーバ108に対して着脱自在なICカード109の内部に設けられている。また、ICカード制御部85は、イメージサーバシステム108の画像ファイル更新部86'の内部に設けられている。

【0058】編集後の画像ファイルと編集履歴のデータとは画像ファイル更新部86'のMD作成部87に入力されてハッシュ関数などの所定の関数を用いてMD2が作成される。このMD2はICカード制御部85の制御によりICカード109のMAC作成部88に送られる。MAC作成部88はMD2を秘密鍵 $K_{private}$ （ICカード）を用いて暗号化してMAC2を作成する。このMAC2はICカード制御部85の制御によりヘッダ記録部89に送られて図9の（D）または（E）に示すようなフォーマットで画像ヘッダに記録される。なお、第5実施形態のようにICカード109に個人認証用情報を格納しておき、これを読み出して編集履歴中に記録

14

するようにしてもよい。

【0059】上記した第6実施形態によれば、第5実施形態の効果に加えて、暗号化鍵の管理と暗号化の処理をICカードのような着脱自在な記憶媒体で構成し、画像の編集や編集履歴データの作成などの他の機能をソフトウェアで構成するようにしたので、低コストでイメージサーバを構築できる効果を有する。

【0060】以下に本発明の第7実施形態を説明する。第7実施形態は復号化鍵取得・登録システムに関し、公開鍵サーバ機構と改竄検査装置、イメージサーバの公開鍵取得・登録機構とから構成される。本実施形態で用いられる暗号化としての秘密鍵と復号化鍵としての公開鍵とは図13（A）に示すように、メーカーにより、デジタルカメラ220やイメージサーバ221、ICカード222などの装置の製造時に鍵生成機構120により生成され、このうち、秘密鍵は装置に内蔵、登録される。登録後、この秘密鍵は直ちに安全かつ確実な方法で消去される。

20 【0061】また、公開鍵は装置に固有の識別子としてのシリアル番号と対応させて図13（B）に示す公開鍵サーバ機構110の鍵登録部202により記録媒体203に記憶される。

【0062】改竄検知装置、イメージサーバの公開鍵取得・登録機構111が例えばデジタルカメラ220によって撮影された画像に対する改竄検知を行う場合には、公開鍵取得部212から装置のシリアル番号が通信制御部211、通信回線210、209、通信制御部208を介して鍵検索部204に送信される。鍵検索部204は装置のシリアル番号に対応する公開鍵を記憶媒体203から読み出してMD作成部205に送る。MD作成部205はハッシュ関数等の所定の関数を用いてMDを作成してMAC作成部206に送る。MAC作成部206は秘密鍵メモリ207にあらかじめ記憶されている秘密鍵を用いてMACを作成し、公開鍵とともに通信制御部208、通信回線209、通信回線210、通信制御部211を介して公開鍵取得部212に送る。公開鍵取得部212は取得した公開鍵と装置のシリアル番号とを公開鍵登録部214に送る。公開鍵登録部214は当該公開鍵と装置のシリアル番号とを公開鍵メモリ213に登録する。

40 【0063】同時に、公開鍵取得部212から公開鍵のデータがMD作成部216に、MACが復号化部217に送られる。MD作成部216はハッシュ関数等の所定の関数を用いてこの公開鍵のデータからMDを作成する。復号化部217は公開鍵メモリ218に記憶されている鍵管理サーバの公開鍵 K_{public} （鍵管理サーバ）を用いてMACを復号化することによりMD'を作成する。比較一致部215はMDとMD'とを比較して一致するか否かにより改竄を検知する。ここでのMACの検証は通信手段で得られたカメラやイメージサーバの公開

50

(9)

15

鍵が、正当な鍵管理サーバから取得されたものか、さらには、通信の途中で改竄されていないかを確認するのが目的である。

【0064】なお、公開鍵サーバ110に登録されている公開鍵は郵送等の安全な手段でユーザに届けるようにしてもよい。上記した第7実施形態によれば、改竄検知用データの復号化鍵は復号化鍵（公開鍵）サーバに装置のシリアル番号を送ることで取得することができる。したがって、例えば復号化鍵サーバをインターネットから利用できる場合には、カメラのシリアル番号を元に世界中どこからでも改竄検知用データを取得することができる。

【0065】以下に本発明の第8実施形態を説明する。第8実施形態は多重解像度画像の改竄防止に関するものである。ドキュメントファイルは一部を改変した場合、文章が繋がらなくなったり、意味が変化してしまい、元のファイルとは内容が異なってしまう。それに対して画像データは冗長性が高いため、解像度の変更など、多少の編集を行っても被写体は認識できることが多い。そのため、画像を利用する側では、撮影時の画像サイズでは必要以上の大きさであり解像度を落としたいことや不要な部分が写っているため、必要な部分のみを切り出したいことがある。ところが、通常は改竄防止用イメージサーバを用意し、その内部で画像を編集してMACを再度付加しなくてはならない。

【0066】そこで、第8実施形態では、上記の問題を解決するために、改竄防止カメラの画像を、多重解像度画像を保持するフォーマットで保存するようにする。図14は本発明の第8実施形態の構成を示す図である。デジタル証拠カメラ部112において、撮像手段60により被写体を撮像することにより得られた画像データは画像メモリ6に記憶される。次にこの画像データは画像縮小部300に入力されて、複数種類の解像度の画像に変換される。このとき、ユーザがMAC作成解像度指示部302を通じて改竄を保証したい最小の解像度を指定すると、これがファイリング管理部13を介してMD作成部9に送られる。MD作成部9ではハッシュ関数などの所定の関数を用いてMDを作成する。

【0067】一方、秘密鍵メモリ10には、カメラ固有のデータメモリ301に記憶されたカメラ固有のデータと、ICカード制御部41の制御により個人認証用ICカード40から読み出した個人認証用の情報とから作成された秘密鍵が記憶されている。MAC作成部11ではこの秘密鍵を用いてMD作成部9で作成されたMDを暗号化してMACを作成してファイリング管理部13に送る。ファイリング管理部13は複数種類の解像度の画像データを1つのファイルにまとめ、さらに上記の指定された解像度のデータから作成したMACを当該画像データに付加して記憶媒体制御部15の制御により記憶媒体17に保存する。

16

【0068】図16は本実施形態の画像データファイルについて説明するための図である。図16に示すように、高解像度から低解像度への変換はあらかじめ規定しておく。MAC作成解像度指示部302で指示された、改竄防止を保証する解像度のデータからMACを作成し、画像データのヘッダまたは別のMAC管理ファイルに記録する。

【0069】一方、改竄検査装置113では、記憶媒体制御部18の制御により記憶媒体17からMAC及び画像データを読み出してファイリング管理部19に送る。ファイリング管理部9ではMACを復号化部21に、画像データを画像メモリ303に送る。復号化部21では公開鍵を用いてMACを復号化することでMD1を作成する。また、画像メモリ303に記憶された画像データは画像縮小部304で所定の縮小方法で縮小された後、MD作成部22に送られてハッシュ関数などの所定の関数を用いてMD2が作成される。一致比較部23ではMD1とMD2とを比較することにより画像データが改竄されたか否かを判断する。

【0070】以下に図15を参照して本発明の第9実施形態について説明する。第9実施形態は多重解像度の画像を保持し、かつ、各解像度の画像は一定サイズの小ブロックを単位として格納されている画像フォーマットの改竄を防止することを意図している。この画像フォーマットで小ブロックを単位として格納している理由は、画像の一部を高速に参照できるようにするためである。

【0071】デジタル証拠カメラ114の作用は上記したデジタル証拠カメラ112の作用と同じであるが、この実施形態では画像縮小・分割部305を有し、ここで複数の解像度の画像を作成するとともに、図17に示すように一定の大きさのブロック単位に画像を分割する。ファイリング管理部13では、各小ブロック毎にMACを作成し、小ブロック毎のヘッダにMACを書き込む。MAC付きの画像ファイルは記録媒体制御部15の制御により記憶媒体17にオリジナル画像として記憶される。

【0072】撮影時、画像の撮影範囲全体や解像度が必要ないユーザは、一般のPC115内で編集ソフトウェア306を利用して記憶媒体17から読み出したオリジナル画像から必要な部分の切り出しや必要な解像度の画像を作成する。ユーザは必要な画像部分の位置、サイズ、解像度などを編集パラメータ307として画像編集部306に入力する。ファイリング管理部13では、対応する解像度の画像から、対応する位置の画像ブロックを抽出し、別の画像ファイルに保存する。

【0073】改竄検知装置116により改竄を検査するときには、記憶媒体制御部18の制御により記憶媒体17からファイリング管理部19に編集済み画像を読み出す。改竄検知部308では編集済み画像に対して改竄検知が行われる。このとき、もともと小ブロック毎に付加

(10)

17

されていたMACをそのまま新しいファイルに付加しておけば、改竄防止イメージサーバを用意しなくとも、ユーザは画像に証拠性を持たせたまま、画像の領域切り出しや解像度の変更といった編集作業を行うことができる。また、コントラスト強調、平滑化などのフィルタ処理を行う場合には、画素値そのものを変更せずに、フィルタ処理の手順を記録したデータを付加すれば、フィルタ処理画像に関してもオリジナル画像の保証が可能になる。

【0074】なお、上記した具体的実施形態には以下のような構成の発明が含まれている。

1. カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、からなることを特徴とするデジタル証拠カメラシステム。

（作用効果）本発明によれば、画像データからカメラ内の暗号化鍵を用いて改竄検知用データを作成し、この改竄検知用データを前記暗号化鍵に対応する復号化鍵を用いて復号化することにより、画像データが改竄されているかどうかを確認できる。これにより、従来フィルムを用いて撮影された画像に比べ、劣るとされていたデジタル画像の証拠能力を高めることができる。

【0075】また、改竄検知用データを作成するための暗号化鍵は、カメラ利用者を含め外部に絶対に漏洩することがあってはならないが、本発明では改竄検知用データを作成するための暗号化鍵は、あらかじめカメラ内に格納されているため、暗号化鍵をハード的に極めて高いセキュリティレベルで管理できる。

2. 前記暗号処理部は、前記画像データに所定の関数を適用して得られたデータを前記暗号化鍵を用いて暗号化することにより前記改竄検知用データを作成することを特徴とする構成1記載のデジタル証拠カメラシステム。

（作用効果）画像データに対する改竄の程度が少なくても変化が大きく現れるように、所定の関数（例えばハッシュ関数）を適用して得られたデータに対して暗号化を行なうことにより改竄検知用データを作成したので、より確実に改竄検知を行なうことができる改竄検知用データを提供することができる。

3. 前記改竄検知部は、前記画像データに前記所定の関数を適用して得られたデータと、前記改竄検知用データを前記復号化鍵を用いて復号化して得られたデータとを比較することにより、前記画像データが改竄されたか否かを検知することを特徴とする構成2記載のデジタル証拠カメラシステム。

18

（作用効果）前記改竄検知用データを用いているので、より確実に改竄検知を行なうことができる。

4. 前記暗号処理部は、前記暗号化鍵と、個人認証用データとに基づいて前記改竄検知用データを作成することを特徴とする構成1記載のデジタル証拠カメラシステム。

（作用効果）画像データの改竄検知用データ作成時に、個人認証用の情報も付加することで、画像の改竄の有無のみならず、画像撮影者も特定することができる。

5. 前記暗号処理部は、前記画像データから、前記暗号化鍵を用いて第1の改竄検知用データを作成し、前記画像データから、前記個人認証用データを用いて第2の改竄検知用データを作成して、前記第1及び第2の改竄検知用データを合わせて前記改竄検知用データとすることを特徴とする構成4記載のデジタル証拠カメラシステム。

（作用効果）画像データから作成した第1の改竄検知用データと、撮影者の個人認証用データから作成した第2の改竄検知用データとをあわせて改竄検知用データとして用いるので、前記第2の改竄検知用データを電子メールや電子商取引など他の情報システムで用いられている電子署名と同様に応用することが可能であり、電子公証局や電子商取引などの社会基盤的な情報システムと連携が取れたデジタル証拠カメラシステムを構築することもできる。

6. 前記個人認証用データ及び前記暗号化鍵を記憶する記憶部と、前記個人認証用データから第2の改竄検知用データを作成する第2の暗号処理部とを備え、この前記第2の暗号処理部を前記カメラに対して着脱自在に構成したことを特徴とする構成4記載のデジタル証拠カメラシステム。

（作用効果）個人認証用データと暗号化鍵を記憶し、第2の改竄検知用データを作成する第2の暗号処理部を、カメラに対して着脱自在な媒体（ICカード等）に設けたことで、この媒体を携帯しておけば、普段利用していない他人のカメラを用いた場合でも、確実に個人の認証及び撮影した画像の改竄の有無を確認することができる。

7. 前記暗号処理部は、前記画像データと前記個人認証用データとを合わせたデータから、前記暗号化鍵を用いて前記改竄検知用データを作成することを特徴とする構成4記載のデジタル証拠カメラシステム。

（作用効果）撮影者の個人認証用の情報として、画像データと個人認証用データを合わせたデータから、前記暗号化鍵を用いて改竄検知用データを作成する方法の場合には、1つの改竄検知データで、画像データの改竄と撮影者の個人認証用データの改竄を検知できる。撮影者の個人認証用データが改竄されてなければ、個人認証用データから撮影者を特定できる。

8. カメラにより被写体を撮像して得られた画像データ

(11)

19

の改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、からなり、前記カメラは、前記画像データが改竄されたか否かを検知する改竄監視モードに加えて、前記カメラから前記改竄検知部へ転送される画像データに対する暗号化を行なうセキュアモードと、電子透かしデータを画像データに埋め込む電子透かしモードと、セキュリティ機能を働かせないで通常の撮影を行なうノーマルモードとを有し、これらのモードから少なくとも1つの所望のモードを選択するためのモード選択部を有することを特徴とするデジタル証拠カメラシステム。

(作用効果) カメラに各種モードの選択機能を備えることで、カメラの使用目的に応じた所望の機能を設定できる。例えば、スナップ画像を撮る時にはノーマルモードで撮影し、証拠画像となるものを撮影する場合には改竄監視モード、また、著作権を守りたい画像に対しては電子透かしモードで撮影することで著作権を守ることができる。さらに、機密性の高い画像を撮影し、画像ファイルを安全に送信したい場合には、セキュアモードを選択することで、データの保存や送信を安全に行うことができる。また、複数のモードを組み合わせることで上記の効果から、1台のカメラを様々な用途に利用することが可能となる。

9. 装置に固有の識別子と、この識別子に対応して生成された第1の暗号化鍵に対応する第1の復号化鍵とをあわせて記憶する復号化鍵記憶部と、前記第1の復号化鍵に関する改竄検知用データを第2の暗号化鍵を用いて作成し、この改竄検知用データと前記第1の復号化鍵とあわせて出力する復号化鍵出力部と、を備えた復号化鍵サーバと、前記復号化鍵サーバから通信手段等を介して取得した前記第1の復号化鍵を記憶する復号化鍵記憶部と、前記第2の暗号化鍵に対応する第2の復号化鍵を用いて、通信手段等を介して前記復号化鍵サーバから供給された前記改竄検知用データを復号化し、この復号化の結果に基づいて前記第1の復号化鍵が改竄されたか否かを検知する改竄検知部と、を備えた復号化鍵取得・登録システム。

(作用効果) 本発明によれば、改竄検知用データの復号化鍵は復号化鍵サーバに装置のシリアル番号を送ることで取得することができる。したがって、例えば復号化鍵サーバをインターネットから利用できる場合には、カメラのシリアル番号を元に世界中どこからでも改竄検知用データを取得することができる。

20

10. 画像データの改竄を検知するとともに、画像データの編集を行なうデジタル画像編集システムであって、画像入力部を介して入力された画像データをファイリング管理するファイリング管理部と、前記画像データにあらかじめ付与された第1の改竄検知用データを、この改竄検知用データを作成する際に用いた暗号化鍵に対応する復号化鍵を用いて復号化するとともに、この復号された第1の改竄検知用データと前記画像データとを比較することにより画像データの改竄状態を検知する改竄検知部と、前記画像データに対し、各種の画像処理を施す画像編集部と、前記画像編集部によって各種画像処理を施された編集済み画像データと前記画像編集部による編集履歴のデータから、前記暗号化鍵とは別の暗号化鍵を用いて第2の改竄検知用データを作成し、これを前記編集済み画像データに付加する画像ファイル更新部と、からなることを特徴とするデジタル画像編集システム。

(作用効果) 本発明によれば、画像データと編集履歴とをあわせて改竄検知用データを作成しているので、元の画像に対しどのような編集処理が施されたのかを確認でき、さらに、当該システム以外で画像編集処理が施されているかどうかを検知することができる。

11. 前記画像ファイル更新部は、デジタル画像編集システムに対して着脱自在であり、前記個人認証情報及び前記別の暗号化鍵を記憶するとともに、前記個人認証情報に前記別の暗号化鍵を用いて前記第2の改竄検知用データを作成することを特徴とする構成10記載のデジタル画像編集システム。

(作用効果) 暗号化鍵の管理と暗号化の処理をICカードのような着脱自在な記憶媒体で、画像の編集や編集履歴データの作成などの他の機能をソフトウェアで構成することで、低コストでイメージサーバを構築できる。

12. 前記編集履歴に個人認証情報をあわせて記録したことを特徴とする構成9記載のデジタル画像編集システム。

(作用効果) 画像編集履歴のデータも含めた画像データに、個人認証用の情報を含めることで、画像を編集した人物を特定することができる。

13. 前記画像入力部は、外部記憶媒体に記憶された画像データを、前記画像ファイリング部に直接接続(ケーブル、IrDA)、又は、通信回線を介して接続することにより入力することを特徴とする構成9記載のデジタル画像編集システム。

(作用効果) イメージサーバの画像ファイリング部に、シリアルケーブル、SCSI、IrDA等の直接接続の端子や、イーサネット等のネットワーク接続の端子を備えることで、外部装置から容易に画像ファイルを入力することができる。

14. 前記画像データは、解像度の互いに異なる複数の画像データを組にして記憶した多重解像度画像データであり、前記暗号処理部は、前記改竄検知用データを作成

(12)

21

するため、前記多重解像度画像データのなかから所望の解像度を有する少なくとも一つの画像データを選択する選択部を有することを特徴とする構成1又は10記載のデジタル証拠カメラシステム。

（作用効果）記録時に改竄検知を保証する解像度を規定することにより、画像を利用するユーザーは撮影時の解像度に依存しないで所望の解像度画像を利用することが可能となる。

15. 前記画像データは、解像度の互いに異なる複数の画像データを組にして記憶した多重解像度画像データであり、前記多重解像度画像データ内の各画像データは、所定の小ブロックを単位として記憶されており、前記暗号処理部は、前記小ブロック単位で、前記改竄検知用データを作成することを特徴とする構成1又は10記載のデジタル証拠カメラシステム。

（作用効果）小ブロック毎に改竄検知データを付加することにより、専用のサーバを用意することなく、切り抜きのような画像編集を行なった画像に対しても改竄検知をすることができる。

【0076】

【発明の効果】本発明によれば、デジタル画像の証拠能力を高めることができ、暗号化鍵を極めて高いセキュリティレベルで管理することができるデジタル証拠カメラシステム、復号化鍵取得・登録システムを提供することができ、さらに、画像の性質上必要となる圧縮や領域切り出し、キャプションの挿入等の編集を施してもデジタル画像の証拠能力を保てるデジタル画像編集システムを提供することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図2】画像データにMACが付加されるまでの手順を示す図である。

【図3】本発明の第2実施形態に係るデジタル証拠カメラの構成を示す図である。

【図4】本発明の第3実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図5】画像データに個人認証用データとMACが付加されるまでの手順を示す図である。

【図6】本発明の第4実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図7】画像データにMAC1及びMAC2が付加されるまでの手順を示す図である。

【図8】本発明の第5実施形態に係るイメージサーバシステムの構成を示す図である。

【図9】第5実施形態の作用を説明するためのフローチャートである。

22

【図10】本発明の第6実施形態に係るイメージサーバシステムの構成を示す図である。

【図11】第5実施形態のイメージサーバシステムの構成例を示す図である。

【図12】第6実施形態のイメージサーバシステムの構成例を示す図である。

【図13】本発明の第7実施形態に係る復号化鍵取得・登録システムの構成を示す図である。

【図14】本発明の第8実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図15】本発明の第9実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図16】第8実施形態に係る画像データファイルについて説明するための図である。

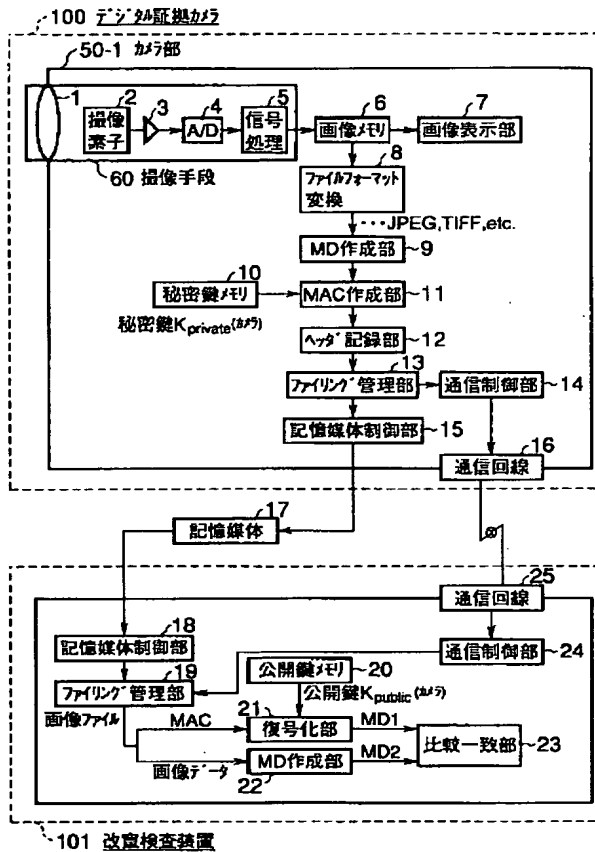
【図17】第9実施形態に係る画像データファイルについて説明するための図である。

【符号の説明】

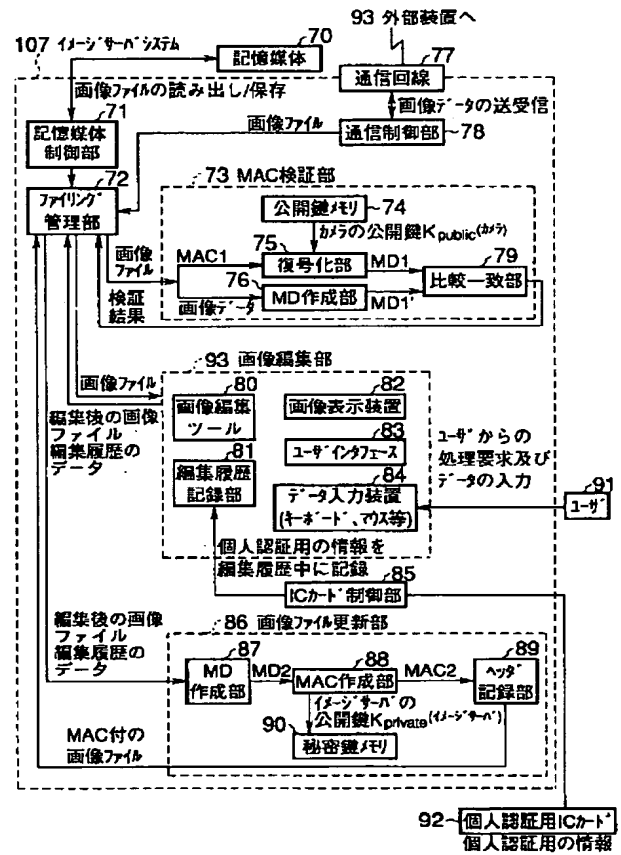
- 1…撮像レンズ、
- 2…撮像素子、
- 3…増幅部、
- 4…A/D変換部、
- 5…信号処理部、
- 6…画像メモリ、
- 7…画像表示部、
- 8…ファイルフォーマット変換部、
- 9…MD作成部、
- 10…秘密鍵メモリ、
- 11…MAC作成部、
- 12…ヘッダ記録部、
- 13…ファイリング管理部、
- 14…通信制御部、
- 15…記憶媒体制御部、
- 16…通信回線、
- 17…記憶媒体、
- 18…記憶媒体制御部、
- 19…ファイリング管理部、
- 20…公開鍵メモリ、
- 21…復号化部、
- 22…MD作成部、
- 23…比較一致部、
- 24…通信制御部、
- 25…通信回線、
- 50-1…カメラ部、
- 60…撮像手段、
- 100…デジタル証拠カメラ、
- 101…改竄検査装置。

(13)

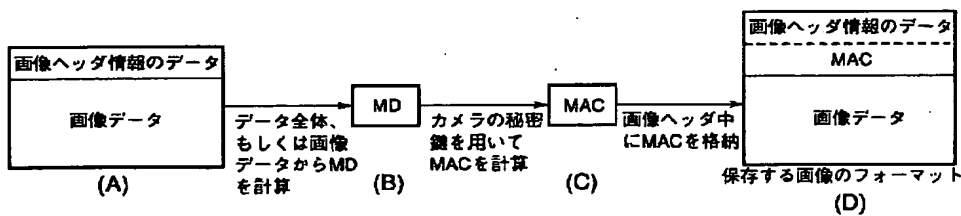
【図1】



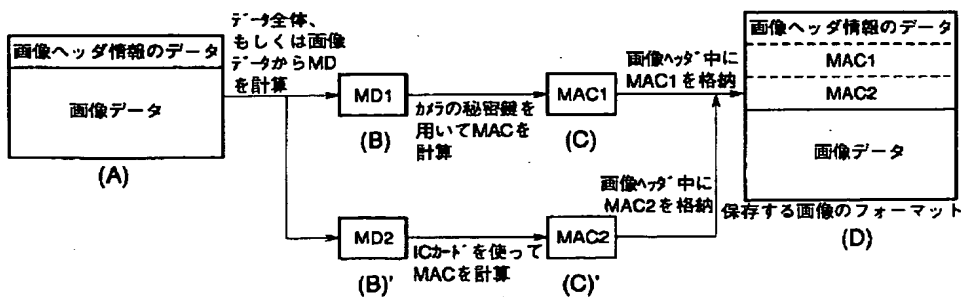
【図8】



【図2】

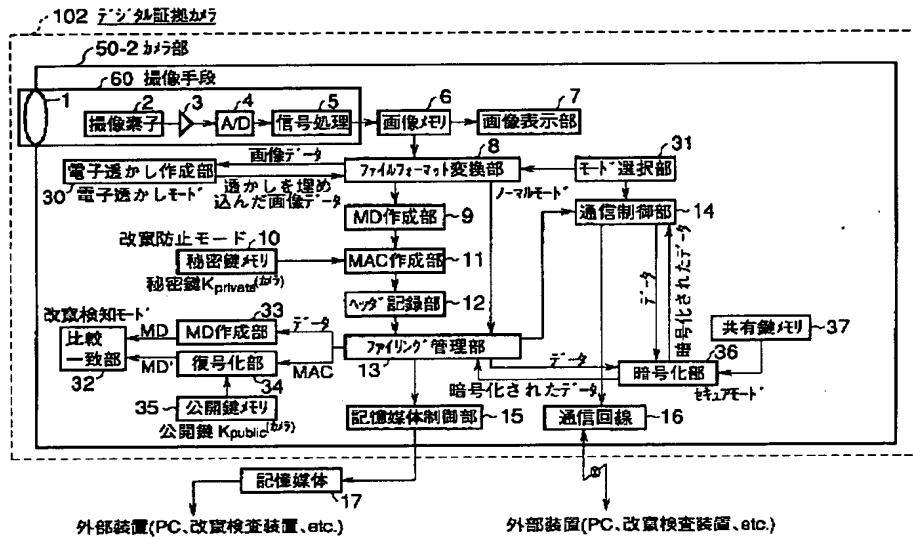


【図7】



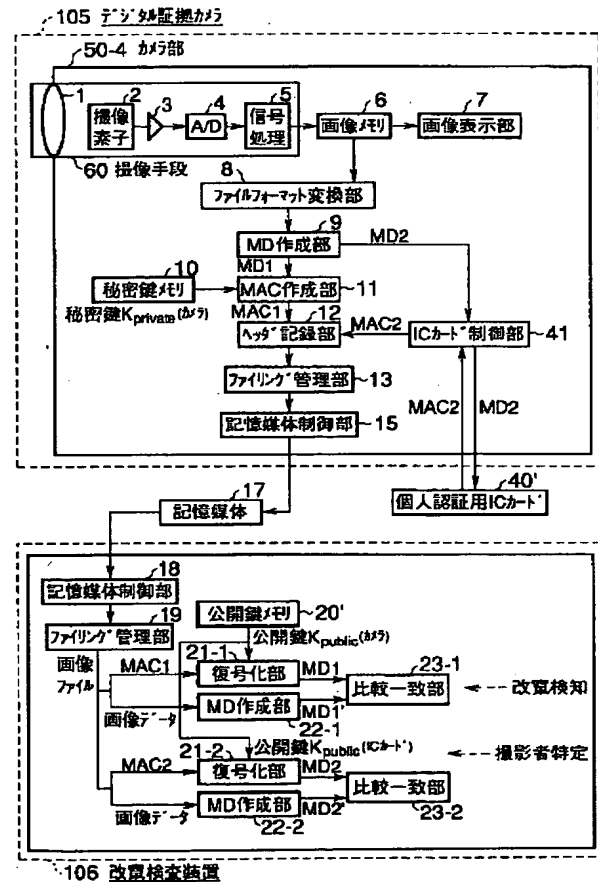
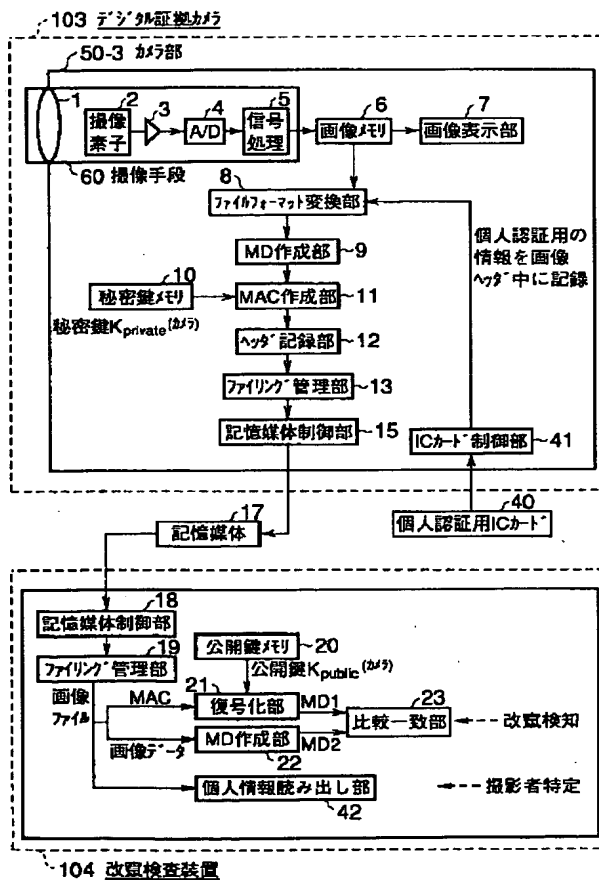
(14)

【図3】



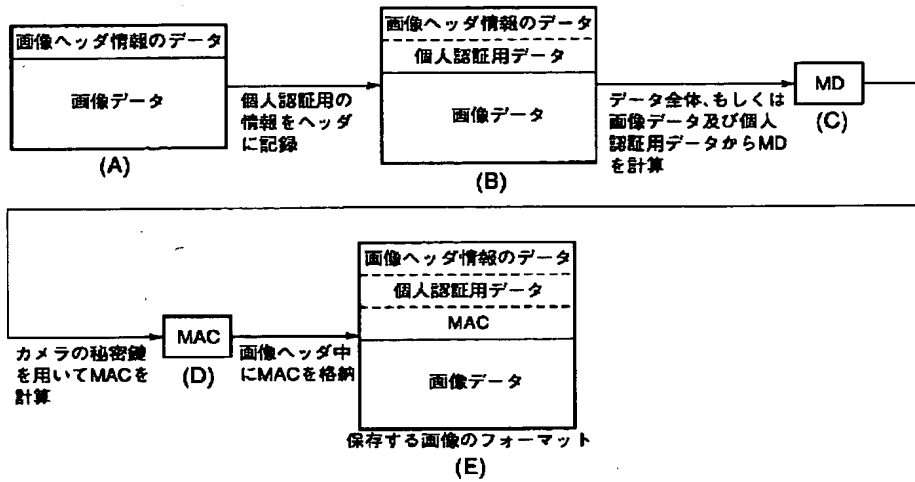
【図4】

【図6】

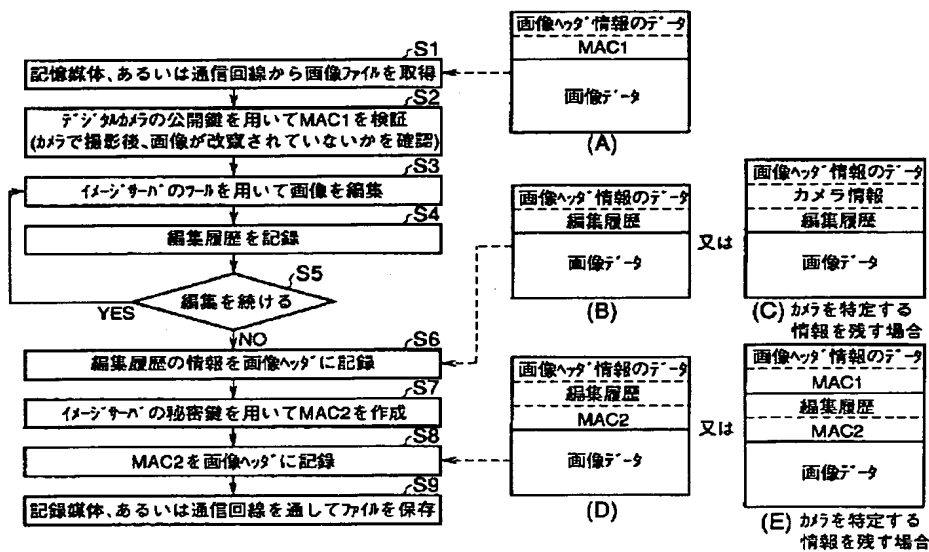


(15)

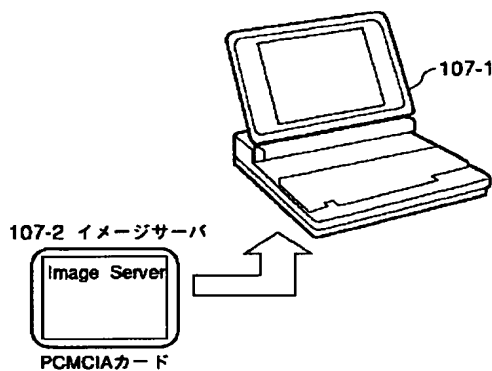
【図5】



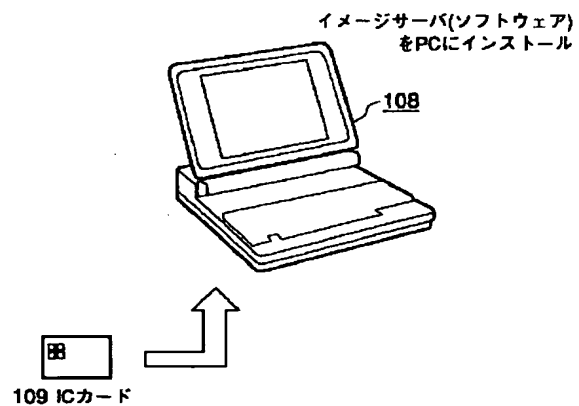
【図9】



【図11】

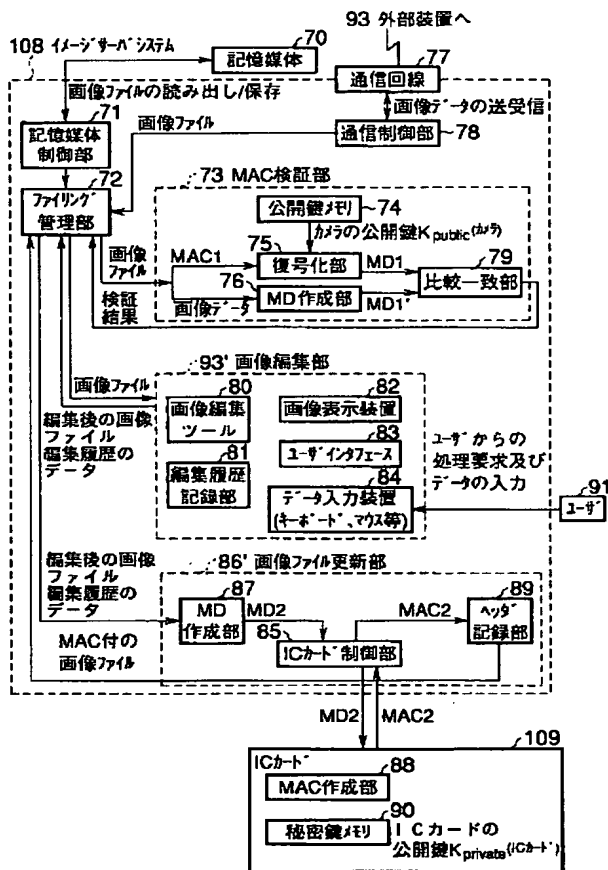


【図12】

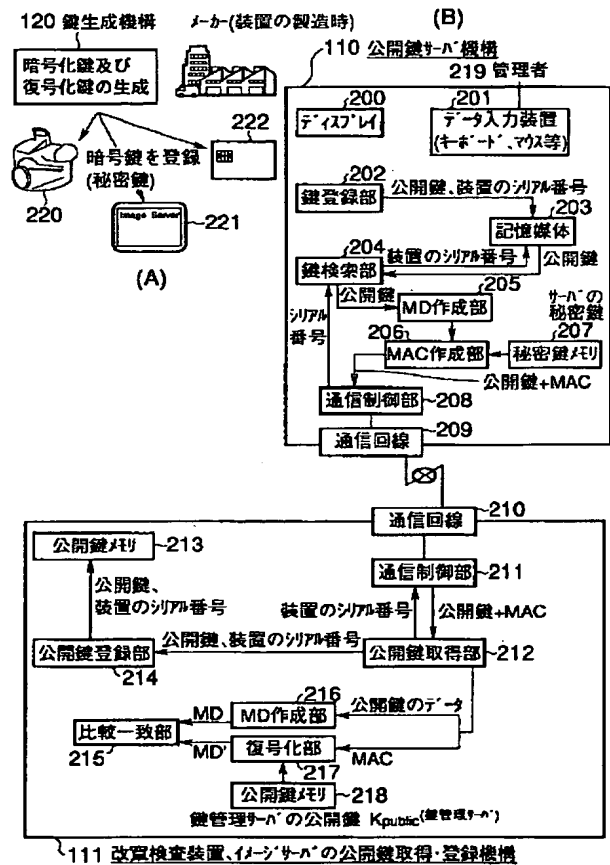


(16)

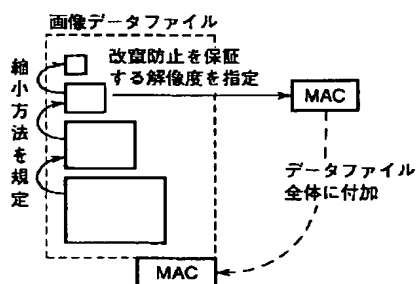
【図 10】



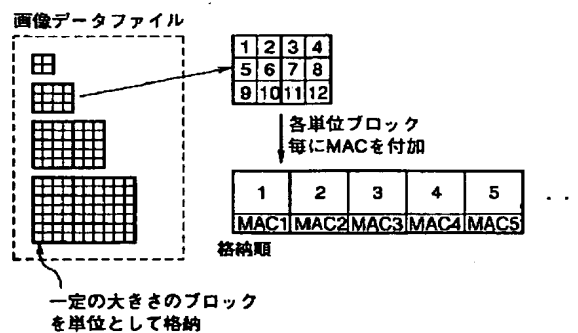
【図 13】



【図 16】



【图 17】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.